PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
G06F 17/60, G06K 5/00, 19/06, 19/07, H04L 9/00, 17/02, H04K 1/00

A1

(11) International Publication Number: **WO 00/26838**

(43) International Publication Date: 11 May 2000 (11.05.00)

(21) International Application Number: PCT/US99/25584

(22) International Filing Date: 1 November 1999 (01.11.99)

(30) Priority Data:
09/184,350 2 November 1998 (02.11.98) US

(71) Applicant: SMARTDISK CORPORATION [US/US]; 3506 Mercantile Avenue, Naples, FL 34104-3310 (US).

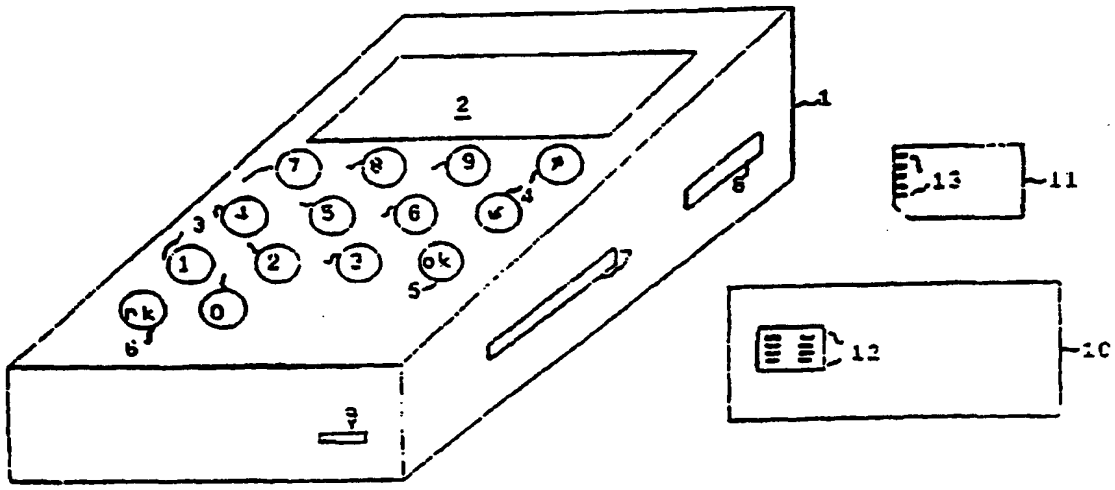
(72) Inventor: EISELE, Raymund; Ferdinand-Abt-Strasse 1, D-65510 Idstein (DE).

(74) Agent: NUSBAUM, Mark, E.; Nixon & Vanderhye P.C., Suite 800, 1100 North Glebe Road, Arlington, VA 22201-4714 (US).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: HOME POINT OF SALE (POS) TERMINAL AND ELECTRONIC COMMERCE METHOD



(57) Abstract

A home point of sale (POS) terminal device provides for enhanced security of electronic commerce transactions.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

HOME POINT OF SALE (POS) TERMINAL AND ELECTRONIC COMMERCE METHOD

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is related to the following application and patent, the subject matter of both being hereby incorporated by reference:

pending application 09/086,677 (Atty Dkt. SMD-0011) filed May 29, 1998, entitled "SMART-CARD AND MEMORY MODULE ADAPTER"; and

U. S. Patent 5,584,043 entitled "APPARATUS HAVING A SMART CARD ACCOMMODATED BY A DISKETTE FRAME CONTAINING PROCESSOR MEMORY AND BATTERY POWER FOR INTERFACING WITH A STANDARD DISKETTE DRIVE."

BACKGROUND OF THE INVENTION

1. Field of The Invention

The present invention relates generally to the field of computer devices, and in particular, to a home point of sale (POS) terminal which is operational to facilitate electronic commerce in conjunction with a personal computer (PC) over the Internet, for example.

2. Background Information

SmartCards and the like are known and have been used for some time in electronic financial transactions, such as making purchases at store-based point-of-sale (POS) terminals, or obtaining cash from automatic teller machines (ATM's). To provide a degree of security, personal identification numbers (PIN's) are generally

required to use such SmartCards. The term SmartCard or "smart-card" as used herein refers to a generally business-card-sized device having a plastic or otherwise semi-rigid/semi-flexible carrier substrate with data storage capability, and which may have processing electronics disposed thereon, such as an ATM card, a patient information card, an electronic cash card, a bank debit card, a FlashPROM card, a credit card, or the like. Sometimes the storage capabilities of such cards are limited to a magnetic strip, while other cards may have several megabytes of electronic memory storage. Such cards are sometimes referred to generically as transaction cards herein. There are also a number of known card communication standards and interfaces to which many cards and associated reading/writing devices adhere. Some cards use electrical contacts while others use magnetic or electrostatic means of communication with associated reading/writing devices. Suffice it to say that there are a variety of cards and devices for reading and/or writing data thereon in usage today.

The variety of transaction cards and associated read/write devices is exemplified by the following publications, the subject matter of which is hereby incorporated by reference. Ishii et al. (5,541,985) disclose a portable electronic device having an external input/output unit and power source integral therewith. An IC card is read from and/or written to with the device which is provided with a control terminal through which power can be turned on/off based on a signal from a portable phone unit. Marceau et al. (5,491,326) disclose a vend card transaction terminal and an associated computer device for implementing inventory and accounting functions. Roberts et al. (5,438,184) disclose a paystation device adapted to be

coupled to a transaction terminal (POS) for carrying out a transaction between a seller and a buyer using a smart card having a cash token value stored therein. Takahashi (5,406,604) discloses an IC card and a portable terminal. Oogita (5,227,615) disclose a portable terminal device having a first interface for a first information exchanging card and a second interface for a second information exchanging card. Johnson et al. (5,149,945) disclose a method a coupler for interfacing a portable data carrier with a host processor, such as a personal computer or point of sale device. Hoppe (5,068,894) discloses a method of generating a unique number for a smart card and its use for the cooperation of the card with a host system. Masuzawa et al. (5,015,830) disclose an electronic card reading device. Hirokawa (4,672,182) disclose a memory card. Dreifus (4,575,621) discloses a portable electronic transaction device and terminal therefore. DE 3528199 discloses a check card system. Oki Electric Industry Co., Ltd. ("OAP Releases Valu-Checker PLUS™ ") announces a personal smart card reader with optional PC Connect adapter to connect to a personal computer through a serial port.

Recently, information exchange and commerce using personal computers , has become increasingly popular, in particular, over the Internet connecting through a network of other computers to a business' World Wide Web (WWW) site. As generally understood by those skilled in the art, the Internet is a global network connecting millions of computers. An internet (lowercase "i") is a network of computers, usually a collection of networks interconnected with routing computers. The Internet (uppercase "I") is the largest internet in the world. It has a three-level

hierarchy composed of backbone networks, mid-level networks, and stub networks. The Internet is a multi-protocol internet using packet-switching between host computers/nodes. Computers on the Internet have an Internet address that uniquely identifies them. The World Wide Web (WWW) is a system of Internet servers that support specially formatted documents, i.e., formatted in a language called HyperText Markup Language (HTML), that supports links to other documents, as well as graphics, audio and video files. There are several application programs called Web browsers which facilitate access to the WWW, e.g., Netscape Navigator and Microsoft's Internet Explorer.

Unfortunately, computer viruses and so-called "Trojan horse" programs can be spread easily and rapidly through this relatively new communications medium, and this presents significant security problems for internet commerce. A computer virus is a program which hides inside another computer program and waits for an opportunity to carry-out its nefarious mission. In general, a Trojan horse program is a program that carries within itself a means to allow the creator of the program access to the system using it. Such a program could, for example, watch for secret information, such as a PIN number entered on a keyboard during an internet credit-card transaction, capture it, and e-mail it to the program's originator for misuse.

Further, when one communicates with a business' Web site, referred to herein as a "virtual shop" on the Internet, there is the question: Is the dealer with which one is communicating really the one which is shown on the personal computer's (PC) display, or an imposter? To be sure of communicating with the correct dealer, encryption and decryption technology has been used to provide a

digital signature of the dealer with a certificate of authenticity from a Certificate Authority. However, a rogue computer program running on the personal computer could deceive a user. In addition, if a users wants to sign a message, there is the question of whether the message being signed is really the message being displayed on the personal computer screen. Again, a rogue program on the personal computer could deceive the user.

Therefore, a need exists for a solution to the security risks and problems caused by rogue programs, such as viruses and Trojan horse programs, in electronic internet commerce.

There is known a so-called "smart-diskette," which is a device having the external shape of a diskette, for example, a standard 3-1/2 inch diskette, and which contains therein, instead of and/or in addition to a magnetic medium (magnetic disk), interface and processing circuitry for providing particular functionality to the device. The circuitry includes an interface for transferring data between other components provided on the device and/or inserted into the device, and a magnetic head of a standard floppy disk drive into which the device can be inserted.

In various forms, the smart-diskette device may include a microprocessor for controlling the device and performing various tasks, such as data encryption and/or compression. On-board memory may be provided as well in the form of, for example, dynamic RAM (random access memory), ROM (read only memory), EEPROM (electronically erasable/programmable read only memory), and/or Flash memory, for storing programs and/or data.

The device circuitry may be provided in the form of discrete components or, advantageously, as a single integrated circuit (IC), in particular, as an application specific integrated circuit (ASIC).

U. S. Patent No. 5,159,182, and copending application S. N. 08/420,796 (Atty Docket No. LWBR 0006C1) hereby incorporated by reference, disclose embodiments of a smart-diskette insertable element with magnetic interface, processor, power supply and optional display and keypad, designed to be inserted into a standard 3-1/2 inch floppy disk drive of a host computer, i.e., electronic data processing (EDP) equipment, such as a desk-top personal computer (PC) or notebook computer, for example.

An exemplary embodiment of the smart-diskette insertable element disclosed in the above-mentioned patent and application, has a processor with some built-in program/data memory. additional memory for storing data and/or programs, and an interface designed to facilitate the exchange of data between the device and a floppy disk drive read/write head. A driver and coil of the interface convert signals from the processor into the required magnetic form and provide them to the read/write head of a floppy disk drive, and likewise convert signals received from the floppy disk drive read/write head into the required form for use by the processor.

An advantage of the smart-diskette insertable element is that, by virtue of its insertability into the standard and ubiquitous (Bill: i.e., universal, omnipresent, prevalent, extremely common, pervasive, found everywhere, proliferated) floppy disk drive of a personal computer, and its interfaceability therewith, it is possible to carry-out a wide variety of operations with the processor and/or memory on the element,

and interactively with the personal computer. These include but are not limited to encryption and decryption of data and/or verification of user identity. Such operations are accomplished without requiring any specially designed interface or plug-in boards which might be suitable only for use with a limited number of computer systems.

Another advantageous feature of the smart-diskette insertable element is its ability to store additional data and/or programs in on-board and/or add-on memory connected with the on-board processor. This considerably increases the potential areas of application for the element.

The smart-diskette element disclosed in the above patent and application may be equipped with a battery power source supplying power to the electronic components within the element, and/or a generator/alternator, with associated regulator circuitry, driven by the rotation of a floppy disk drive spindle.

As mentioned, the interface of the smart-diskette insertable element is designed to allow data to be exchanged with the read/write head of a floppy disk drive. One way this can be achieved is by locating an electromagnetic component on the element, e.g., one or more coils, to be in the vicinity of the read/write head of the floppy disk drive when the element is inserted into the drive, and which generates magnetic field information functionally the same as that generated by a magnetic disk of a standard floppy diskette. In this way, the interface simulates a magnetic floppy diskette. This property of the interface allows data to be transferred under control of the on-board processor to the EDP equipment (e.g., a personal computer), such as data which enables user identification to be verified, thereby

providing security to the EDP equipment, or any of a number of other operations, as would be recognized by one skilled in the art.

As processor capabilities expand and memory devices with increasing capacity become smaller, the smart-diskette device takes on the potential for more and more useful and varied applications.

Related U. S. Patent 5,471,038, hereby incorporated by reference, discloses a special read/write unit with a read/write head and optional electrical contacts, but without the standard disk driving and head moving parts, for use in a desk-top PC or notebook computer to communicate with a smart-diskette. By eliminating the drive motor and moving read/write heads, a significant amount of energy which would otherwise be expended by the use of such moving parts is conserved.

Further, such a read/write unit, since it eliminates bulky drive and head motors, can be made more compact than a standard floppy disk drive, thereby reducing the overall size and weight requirements for the computer in which it is installed.

Related copending application 08/514,382, hereby incorporated by reference, discloses a pocket interface unit (PIU) for use with a smart-diskette. Pocket calculators and diary devices are known and have gained acceptance with busy executives, for example. However, such devices have numerous limitations and disadvantages. For example, although such devices can interface with a desk-top computer to download application programs and/or data, for example, or to upload data entered on the pocket device to the desk-top computer, to do so currently requires inconvenient cabling, and/or a special interface unit, e.g., PCMCIA, with

associated costs. Some devices use infra-red beams to communicate between the device and the PC, but these are subject to atmospheric and distance limitations, or may be subject to errors due to dust or dirt on a lens, for example.

In addition, such pocket devices are generally limited to a single special application, such as a phone directory, or a golf-handicap calculator, and do not generally provide the range of capabilities of a notebook computer, for example. Pocket-sized pagers and cellular telephones are also known. However, these respective devices do not generally have the capability of functioning as anything except a pager or telephone, that is, they are generally devices which are dedicated to a single function. Therefore, the fully-equipped, fully-functional executive may be burdened by having to carry around a variety of separate devices, which further disadvantageously cannot readily interface with one another.

The PIU, disclosed in the copending application, for use with a smart-diskette, overcomes these and other problems, and provides other advantages over existing technology.

Related U. S. Patent 5,584,043, incorporated by reference, discloses a smart-diskette adapted to receive at least one memory and/or processor card, generically referred to herein as a "smart-card," such as an ATM, patient information, electronic cash card, bank debit card, FlashPROM card, credit card, or the like. For example, Figure 5a of that patent illustrates an embodiment adapted for receiving at least one mini-chip card. This patented device can be used with the recently developed MMC (MultiMediaCard made by Siemens/SanDisk), or the SSFDC also called a SmartMediaCard (SMC, made by Toshiba). These compact memory cards are

referred to generically herein as "memory modules" because of their modular configuration.

The so-called MultiMediaCards (MMC's) provide small, transportable audio/video media storage in the form of a modular card substrate carrying a memory, and an optional processor in some cases, which can be inserted into a number of different media recording/playback devices specifically adapted to receive the MMC's. The MMC memory currently can store, for example, about 16 megabytes of digitized video and/or audio signals, however memory capacities are growing almost daily. Typically, contacts on the MMC are be used to connect and transfer the digitized video/audio to a media recorder or playback device.

Although MMC's and the like are a remarkable technological development, until the advent of the smart-diskette embodiment disclosed in the above mentioned patent, which is adapted to receive at least one modular memory card, such as an MMC, a special add-on device would have been required to load data onto an MMC from a personal computer or vice versa. The smart-diskette provides a convenient low-cost alternative to the special add-on device.

A variety of Flash memory devices (e.g., FlashPROM's) have also become known and are more and more widely used, for example, in digital cameras. The above-mentioned SMC's and other memory modules may use Flash memory or any other type of non-volatile memory available.

Further, to use the MMC's as proposed for storing and playing back high-fidelity musical compositions, a user would need an entirely new recording/playback device designed with a port for interconnecting with the MMC's to make use of them

in their home. In other words, the existing conventional user playback/recording equipment, such as an audio cassette player, does not generally interface with the newly developed MMC's. Therefore, a need existed for an adapter device which could permit use of the new MMC's with the existing conventional electronic equipment, such as home/auto recording/playback equipment. Copending application 09/013,036 (Atty Dkt. SMD-0008), hereby incorporated by reference, meets this need and discloses an adapter for use in adapting a conventional cassette tape playback/recording device with a plurality of Flash memory devices, MMC's, or the like, which store digitized audio, for example. The adapter provides a way of adapting one or more MMC's to conventional recording playback devices, such as a conventional audio or video cassette player. The adapter inserted into a conventional tape device interfaces the tape device with one or more removable storage circuits (e.g., MMC's) which store digital audio and/or video data. By accommodating a number of MMC's at once, a user can advantageously record and/or playback an extended audio or visual work with the adapter.

Of course, MMC's, Flash-memory devices, and the like, can be put to other uses besides storing audio and/or video/image data for use in a home or automobile system. They can be used to store any type of digital data imaginable. The inventive adapter disclosed in the copending application is in the form of a tape cassette, i.e., audio, video, or digital (e.g., DAT). While digital tape drives are available as relatively expensive add-on devices for personal computers, these tape drives are not in as widespread use as the floppy disk drives which are provided with practically every personal computer as a standard feature.

To take further advantage of some of the other possibilities of MMC's, Flash-memory devices, and the like, and to overcome problems in the art, an improved adapter element in the shape of a diskette for insertion into a floppy disk drive, which is designed to receive a plurality of memory modules or cards therein, was developed and is disclosed in copending application 09/021,986 (Atty Dkt. SMD-0010), hereby incorporated by reference.

According to an aspect of that disclosed adapter device, up to 5 MMC's can be inserted at once into respective sockets. Two modules are insertable (which also means removable) at the left edge of the adapter, two at the right of the adapter, and one at the rear (outer) edge of the adapter. The adapter with one or more memory modules is insertable into a floppy disk drive front edge (inner edge) first. Further, the adapter provides for playback of music and/or image data, for example, from one or more memory modules, via the floppy disk drive of a personal computer. Music and/or image data, for example, can be recorded on one or more memory modules via the personal computer floppy disk drive.

Further, the inventor realized that there may be times when it would be advantageous to have a single adapter which could accommodate both a smart-card and at least one memory module simultaneously. For example, should a personal computer user wish to purchase a music selection or picture image, for example, over the Internet using their bankcard (smart-card) for payment, they could do so with a smart-diskette adapter described above which interfaces their personal computer with their bankcard. If the user wanted to download the music or image purchased into a memory module, they could do so with another different smart-

diskette adapter, described above, which interfaces their personal computer with an MMC through the floppy drive.

Related co-pending application 09/086,677 (Attorney Docket SMD-0011), provides a method and apparatus for an adapter which can accommodate both a smart-card and at least one memory module at the same time, and thereby provide the functionality of two different adapters in one, as well as a synergistic enhancement of functionality, thereby providing advantages over the prior adapters. This adapter includes a frame having the shape of a diskette, the frame having at least one first recess for receiving an insertable memory module, and a second recess for receiving an insertable smart-card, the frame having therein interface circuitry providing an interface with a read/write head of a floppy disk drive, the memory module, and the smart-card, when inserted in the respective recesses. The frame has the shape and size of a 3-1/2 inch floppy diskette. The at least one first recess is adapted to receive at least one of a plurality of standard memory modules, the plurality of standard memory modules including multi-media cards (e.g., MMC's), and smart media cards (e.g., SMC's or SSFDC's). The interface circuitry includes respective contacts disposed in respective ones of the first and second recesses which couple with corresponding respective contacts on a respective memory module and smart-card when inserted in the respective recesses; a magnetic interface which is adapted to magnetically couple with a read/write head of a floppy disk drive when the adapter is inserted in the floppy disk drive, and a processor, coupled to the contacts, which is operable to receive and transmit signals to and

from the respective memory module and smart-card through the respective contacts, and to receive and transmit signals to and from the magnetic interface.

That adapter further includes a memory connected to the processor which stores data and/or programs used by the processor, and the magnetic interface includes a magnetic transducer which is operable to send and receive magnetic signals to and from a floppy disk drive read/write head, and a driver/converter connected to the transducer and the processor which is operable to convert signals from the transducer to a form useful to the processor, convert signals from the processor to a form used by a floppy disk drive, and to drive the transducer with the converted signals from the processor. At least one battery is provided on the adapter which is connected to provide power to the interface circuitry, at least one memory module, and at least one smart-card. The memory for the processor stores programming enabling the processor to perform at least one of encryption of data, decryption of data, compression of data, and decompression of data. The processor includes programming to perform interactive password checking to verify authorized use of the adapter and/or the at least one memory module and/or the at least one smart-card.

According to that application (09/086,677, Attorney Docket SMD-001.1), a method of purchasing data, making payment with a smart-card and storing the data to a memory module, via a terminal having a direct access storage device, e.g., a floppy disk drive, includes utilizing the adapter according to the invention having the smart-card and the memory module inserted therein. The terminal is a personal computer which is connected to the Internet for receiving the data therefrom and

making the payment thereto. Electronically purchasing data is facilitated using the disclosed adapter device which is insertable into a terminal direct access storage device, and which accommodates an electronically readable card and at least one memory module therein. In an exemplary method, an electronically readable card and at least one memory module are inserted in the adapter, and the adapter is inserted into a terminal direct access storage device. Upon selecting with the terminal data to purchase having an associated purchase price, a payment amount corresponding to the purchase price is debited from the electronically readable card, and the data to be purchased is stored in the memory module. The terminal device comprises a personal computer, and the method further includes establishing a communications path between the personal computer and a remote location where the data to be purchased is pre-stored. An anti-piracy mechanism to prevent piracy of copyrighted material is included. Encryption, decryption, compression or decompression on the data to be purchased can be performed before storing the data to the memory module. User identification and user authentication prior to debiting a payment amount from the electronically readable card are provided for as well. The electronically readable card may be an electronic cash card having stored thereon an electronic representation of a cash value, and the debiting includes electronically reducing the stored cash value by the payment amount. The electronically readable card may be a credit card, and the debiting including communicating with the credit card issuer to establish a credit card purchase.

That application (09/086,677, Attorney Docket SMD-0011) further discloses a method of access security using an adapter device which is insertable into a terminal

direct access storage device, and which accommodates an electronically readable card and at least one memory module therein, including pre-storing first user data in a memory module, pre-storing second user data in an electronically readable card, inserting the memory module and the electronically readable card into the adapter, inserting the adapter into a terminal direct access storage device; verifying the user data pre-stored in the memory module and the electronically readable card, and permitting or denying access to the terminal device based on a result of the verifying. The permitting access includes permitting an access level corresponding to the user data.

However, the inventor has recognized that, because of the Trojan Horse type of security issues, for example, a need exists for further improvements in this field to overcome a number of issues related to secure use of SmartCards, especially in internet commerce applications. Some applications require that the SmartCard PIN be entered before communicating with the SmartCard chip. If the PIN is entered via the personal computer's keyboard, then there is the possibility that a Trojan horse program with a keyboard grabber could read the secret PIN.

In order to overcome the problems of ensuring against unauthorized discovery of and misuse of PIN's, as well as other security access information related issues, the present invention provides novel solutions in the form of a Home POS Terminal for smart card use and electronic commerce methods, exemplary embodiments of which are described in detail below.

SUMMARY OF THE INVENTION

It is, therefore, a principle object of this invention to provide a secure method of electronic commerce and an apparatus for implementing a Home POS Terminal.

It is another object of the invention to provide a method and apparatus that solves the above mentioned problems so that electronic commerce can be conducted in a more secure fashion.

These and other objects of the present invention are accomplished by the method and apparatus disclosed herein.

The present invention provides an enhancement of the functionality as is described in the related SmartDiskette patent 5,584,043, and in copending application 09/086,677 (SMD 0011). In addition, the present invention provides advantageous new functions, as will be described below.

As mentioned above, some applications require that a user's SmartCard PIN be entered before permitting communication with the SmartCard chip. However, as mentioned earlier, if the PIN is entered via a personal computer (PC) keyboard, then there is the possibility that a Trojan horse program with a keyboard grabber will read the secret PIN. Therefore, according to an aspect of the invention, it is proposed to provide for the entering of the PIN at the Key Pad of a Home POS Terminal connected to the personal computer, and showing the result of PIN verification at the display of the Home POS Terminal.

According to another aspect of the invention, as mentioned above, when communicating with a virtual shop on the Internet, there is the question of whether the dealer or business with which one is communicating is really the dealer or

business which is shown on the PC's display, or an imposter. To be sure of communicating with the correct dealer or business, one requests a digital signature of the dealer with a certificate of authenticity from a Certificate Authority. According to an aspect of the invention, the certificate and dealer signature are advantageously decrypted in a digital signature processor provided in the Home POS Terminal, and the dealer's real identity is shown on the Home POS Terminal display.

According to another aspect of the invention, when one wants debit a certain amount from, e.g., a stored value on a SmartCard, there is the question of whether the debit amount which is shown on the PC's display is really the amount which will be debited from the SmartCard. According to the invention, the amount that will actually be debited from the SmartCard is displayed on the Home POS Terminal display. The user is able to confirm the amount to be debited, with an "OK." Key on the Home POS Terminal, for example, or to reject the amount, with a not OK key, for example.

According to another aspect of the invention, when a user wants to sign a message to be sent, there is again the question of whether the message shown on the personal computer display is really the one which will be signed, in the SmartCard processor or in the digital signature processor, for example. Therefore, according to an aspect of the invention, the message which will actually be signed will advantageously be displayed on the display of the Home POS Terminal. If it is a long message, for example, which cannot be shown in full on the display of the Home POS Terminal, the user can use page-up/page-down keys advantageously

provided thereon. To confirm the message, the user hits an "OK" key and can thereby be sure that "what you see is what you sign" (wysiwys).

Advantageously, protected functions of the Home POS Terminal, such as communication with the Home POS Terminal display and keypad can be "hard coded" in a display driver and key pad driver, respectively. Other functions, such as for an interface driver, can be down-loaded from the personal computer to the Home POS Terminal.

Advantageously, according to another aspect of the invention, there are provided multiple interfaces to connect a Home POS Terminal to a personal computer (PC). Such interfaces may include parallel and serial interfaces, PCMCIA, USB, mouse and keyboard interfaces.

Connector cables with "Y" plugs, for example for the mouse or keyboard of the personal computer, can be used if there are no other connections available. According to an aspect of the invention, a modified keyboard or mouse driver is installed. Usually, such drivers provide for communication between the personal computer and the keyboard or the mouse. However, with the modified drivers, when there is a message to the Home POS Terminal, then according to the invention, communication will be temporarily switched to be set up through the "Y" plug to the Home POS Terminal.

These and other objects of the present invention are accomplished by the method and apparatus disclosed herein.

BRIEF DESCRIPTION OF THE DRAWINGS

The above and other features and advantages of the invention will become apparent from the following detailed description taken with the drawings in which:

Fig. 1 illustrates a Home POS Terminal according to an exemplary embodiment of the invention.

Fig. 2 illustrates the Home POS Terminal according to Fig. 1, as seen from the back.

Fig. 3 illustrates a SmartDisk (SmartDiskette) with insertable SmartCard and MemoryCard.

Fig. 4 shows an alternative embodiment of the Home POS Terminal with connection to the SmartDisk of Fig. 3.

Fig. 5 is a block diagram of the functional component provided in a Home POS Terminal according to an exemplary embodiment of the invention.

Figs. 6a, 6b, and 6c depict a flow chart illustrating the operation of an exemplary embodiment of a Home POS Terminal according to the invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT(S)

The invention will now be described in more detail by example with reference to the embodiment(s) shown in the Figures. It should be kept in mind that the following described embodiment(s) is only presented by way of example and should not be construed as limiting the inventive concept to any particular physical configuration.

Referring to Fig. 1, shown is a Home POS Terminal according to an exemplary embodiment of the invention. The housing 1 of the Home POS Terminal is shown having a generally rectangular shape, however, the invention is not limited to a rectangular housing but can be any shape able to accommodate the constituent components. Mounted at an upper surface of the housing 1 for easy observation is a display 2 which may be any suitable type, for example, a liquid crystal display (LCD) or a plasma-type display, having one or several columns and rows of display elements for displaying alpha-numeric characters, and symbols, or the like. A group of numerical keys 3 is also provided on the upper surface of the housing as shown. Numerical keys 3 include the numbers 0 through 9 as is apparent. Additional keys may also be provided, in particular, page-up and page-down keys 4, an "OK" key 5, and a not OK "NK" key 6, in order to facilitate easy operation of the terminal.

As will be described in more detail later, the page-down and page-up keys 4 are useful for reading messages to be signed, for example, which have more characters than can be displayed at one time on display 2. The functions of the OK key 5 and the NK (not ok) key 6 are to indicate acceptance (OK) or non-acceptance (NK) of a displayed message/operation/quantity, such as a debit amount, for example, during operation.

A slot 7 for a smart-card is provided on a side of the housing as illustrated, for example, or in any other convenient location, and, of course, a smart-card socket or other means (not shown) is disposed within the slot 7 for establishing a communication path between internal circuitry of the Home POS Terminal and a smart-card when inserted therein. While such a means would typically be a number

of mechanical contacts which mate with corresponding contacts on a smart-card to establish an electrical coupling, other types of coupling are possible, e.g., optical, electro-static, or magnetic-based coupling. For the purposes of this disclosure, mechanical contacts are illustrated, but the invention is not limited to such a configuration, and any number of equivalent structures/means for establishing a communication path between the terminal and an inserted card are possible within the spirit and scope of the invention, as would be apparent to one skilled in the art.

Similarly, a slot 8 for a memory card is also provided disposed, for example, on the same side of the housing as the smart-card slot 7, and having a memory card socket or other means (not shown) disposed within the slot 8 for establishing a communication path between internal circuitry of the Home POS Terminal and a memory-card 11 when inserted therein. As with a smart-card mentioned above, a memory-card could be coupled in any number of ways within the scope and spirit of the invention.

A power on/off switch 9 is shown on a front face of the housing 1 of the Home POS Terminal. Power for the Home POS Terminal could be derived from internal batteries, or from an external power supply, for example. As can be imagined, photo-voltaic cells (not shown) could be provided on the top surface of the housing for charging internal batteries, as are often used with pocket calculators, and other compact electronic devices, for example.

At the right-side of Fig. 1, adjacent to the smart-card slot 7, is shown a representation of a typical smart-card 10. Adjacent to memory-card slot 8 is shown a representation of a typical memory card 11. The smart-card 10 is shown having

smart-card contacts 12, while the memory-card 11 is shown having memory-card contacts 13, as examples of ways to establish communication with the terminal. The smart-card 10 and memory-card 11 are shown in schematic form and, as is known in the art, may have any number of shapes and sizes or configurations. A number of these have become "standard" as would be appreciated by one skilled in the art., and the Home POS Terminal would be designed and built to accommodate one or more of these "standard" configurations.

Fig. 2 is a drawing of an exemplary embodiment of a Home POS Terminal, such as is shown in Fig. 1, as seen from the back. The Home POS Terminal housing 1 is advantageously provided with a number of different interface connectors, examples of which include a connector 14 for a USB (Universal Serial Bus) interface, a connector 15 for a Serial Port (e.g., RS-232), a connector 16 for a Parallel Bus Port (e.g., PCI), a connector 17 for a Mouse Port with a "Y" plug cable to connect to a Mouse cable of a personal computer (not shown), reference numeral 18 being the Y-connector portion leading to the Mouse 19, a connector 20 for a Keyboard 22 of a personal computer with a "Y" plug cable to connect to a Keyboard cable, reference numeral 21 representing the Y-connector portion leading to the Keyboard 22, and a connector 23 for a PCMCIA card. The Mouse Port "Y" plug cable, and likewise the Keyboard "Y" plug cable, would be configured to be switchable, under control of modified drivers, between communication with the mouse (Keyboard) and with the Home POS Terminal, as is within the skill of one well-versed in the art. A connection for an optional battery Power Charger 24 is also conveniently provided for at the back of the housing 1, for charging a Battery 25

which powers the circuitry (described later) in the Home POS Terminal housing 1. Of course, other types of power supply configurations are possible, as would be apparent to one skilled in the art.

A connection line (37) leading to a SmartDiskette 26 (also referred to as a SmartDisk herein), such as has been described in the Background section above, is also shown in Fig. 2 and will be described in more detail with reference to Figs. 3 and 4. In particular, Fig. 3: illustrates a representative SmartDiskette 26 which can accommodate an insertable SmartCard 10 and/or MemoryCard 11, and Fig. 4 shows the Home POS Terminal connected thereto. In this alternative embodiment of the terminal, slots for the SmartCard 10 and MemoryCard 11 are provided in the SmartDisk 26 rather than, or in addition to, being provided in the terminal housing 1. As should be apparent, the SmartDisk 26 might be configured differently such that it only accommodates the SmartCard 10, or a MemoryCard (or MemoryCards) 11.

The SmartCard 10 and the MemoryCard 11 shown in Fig. 3 have SmartCard contacts 12 and MemoryCard contacts 13 respectively, which mate with corresponding contact sockets 27 and 36 in the SmartDisk 26. A SmartCard recess 28 is provided for aiding insertion and removal of the SmartCard 10. A MemoryCard recess 30 is likewise provided for aiding insertion and removal of the MemoryCard 11. The SmartDisk 26 has a spindle recess 29 for accommodating a disk drive spindle when the SmartDisk 26 is itself inserted into such a drive. Likewise provided is a slot 31 for the read/write head of such a drive. The SmartDisk 26 may have an optional battery 32 and a power on/off switch 33 which is designed to turn on power

to the SmartDisk circuitry when it is inserted into a disk drive, and turn off power when it is removed from the disk drive.

A transducer 34 is shown adjacent to the slot 31 for receiving and sending magnetic signals with the head of a disk drive. A "MagIC" (Magnetic Interface Chip) 35 is likewise provided which is, for example, an Application Specific Interface Chip (ASIC) custom designed to provide the SmartDisk interface functions. Such a SmartDisk 26 is the subject of the related copending applications mentioned and incorporated herein, and a detailed description thereof is not necessary here for a complete understanding of the invention.

Fig. 4. Shows an embodiment of the Home POS Terminal with a connection 37 to the SmartDisk 26 of Fig. 3. In this illustrated embodiment of the Home POS Terminal, the SmartCard and MemoryCard interfaces are not provided in the terminal housing 1, but are provided instead in the SmartDisk 26. The connector cable 37 between Home POS Terminal housing 1 and the SmartDisk 26 may contain, for example, connections to the socket 27 for the SmartCard contacts 12, the MagIC (Magnetic Interface Chip) 35, the socket 36 for the MemoryCard contacts 13, and the power on/off switch 33. However, instead of a cable 37, the connection could also be established via free-space transmission of information encoded infrared light or radio frequency waves (e.g., microwaves), for example, as indicated by lines 371. Of course in that case, the Home POS Terminal housing 1 and the SmartDisk 26 would be provided with respective free-space transceiver circuitry, as would be apparent to one skilled in the art.

Fig. 5 illustrates a block diagram of exemplary components which would be disposed inside the housing 1 of a Home POS Terminal made according to an embodiment of the invention. This figure also shows schematically the functional connections between the different components. Some of the components illustrated here have already been described in detail with respect to the previous figures, and may only briefly be mentioned again. An interface driver 39 is provided which drives the USB 14, the parallel port 16, the serial port 15, the PCMCIA interface 23, the SmartCard socket 27, the MemoryCard (MC) socket 36, the Keyboard port 20, the MagIC interface 35, and the mouse port 17, as illustrated by the lines connecting these to the interface driver 39. Of course, the block labeled interface driver 39 could be implemented by a single special purpose integrated circuit, a number of integrated circuits, or a combination of discrete interface logic circuits, for example. It should be apparent that the interface driver block 39 could alternatively represent a program module of a microprocessor or microcontroller, for example.

A display driver 40 for display 2, and a keypad driver for the keypad keys 3, 4, 5, 6, are likewise provided, and may be implemented in any of the above described ways. The Interface driver 39, the display driver 40 and the keypad driver 41 provide a connection to the main processor 38, which controls the overall operation of the Home POS Terminal. Power is provided by battery 25, for example, and the SmartDisk switch 33 (see Fig. 3) may be bypassed to provide power to a SmartDisk 26 as indicated by "(33)" at the line between the battery 25 and the processor 38. As described, the switch 33 is configured to power the SmartDisk when it is inserted

in a ubiquitous floppy drive, so in the Fig. 3/4 embodiment, it is bypassed by the signal/connection (33) of Fig. 5.

Associated data and/or program storage 43 is provided in the form of RAM/ROM or other memory, coupled to the processor 38. A digital signature processor 42 is also provided for processing digital signatures, as is understood in the art. Key storage 44 is associated with the digital signature processor 42, as shown. The digital signature processor 42 operates to process digital signatures and certificates in order to verify the authenticity and origination of messages, for example, displaying the result on display 2 by way of the processor 38 and the display driver 40. As is known in the art, digital signal processors (DSP's), for example, are used for the function of digital signature processing. As mentioned earlier, display and key pad drivers (40, 41) may be advantageously hard-coded in the terminal to prevent their compromise by nefarious programs.

Figs. 6a, 6b, and 6c illustrate a Flow Chart of the operation of an exemplary embodiment of the invention. In particular, the flow chart shows the functional flow involved in reading a customer PIN from PIN Pad 3, PIN verification in SmartCard 10, and display of the result on display 2.

In more detail with reference to Fig. 6a, the routine starts with power on 601. At this point 602, the SmartCard (SC) is reset and the ATR (Answer To Reset) is obtained. Next at block 603, the ATR is then checked for protocol, and the protocol information is stored. Flow then proceeds to the decision point 604 where it is determined whether a PIN is required. If the answer is YES, flow proceeds to block 605, where the PIN is requested and read into the terminal. Next, at block 606, the

PIN is sent to the SmartCard (SC) and a response is read. If the response indicates that the PIN is correct (OK) at decision point 607, then flow proceeds to block 608 to display a PIN "OK" message, after which flow goes to entry point "1". If at decision point 607 it is determined that the PIN is not OK, then flow proceeds to block 609 to display a PIN wrong message, after which flow goes to entry point "3" to ask for the PIN again (605). Of course, although not shown, after a certain number of wrong PIN entries, the device could stop and execute additional security routines under the assumption that a security breach is being attempted.

If no PIN is required at decision point 604, or after the PIN has been correctly entered and flow has gone to entry point "1", then the routine proceeds to block 610 to wait for messages from the personal computer (PC) application and test for a reset message at 611. If no reset message is detected at 611, flow proceeds to entry point "2" in Fig. 6b. However, if a reset message is detected at 611, flow proceeds to block 612 where the SmartCard (SC) is reset, and the ATR is obtained and sent to the PC application, after which flow returns to entry point "1".

Shown in Fig. 6b is the flow of operation if the received message is not a reset, i.e., it is a digital signature of a dealer for example. That is, flow has proceeded from decision point 611 in Fig. 6a to entry point "2". Decision point 613 tests for a dealer's signature at 613, and proceeds to 614 if it has determined there is a dealer's signature. In block 614 the certificate will be decrypted (i.e., in Digital Signature Processor 42) to receive the dealer's public key which is then used to decrypt the dealer's signature, and then in block 615, the result (dealer's name) is displayed on display 2, and a user response is awaited, i.e., either an "OK" or a not

OK "NK", as tested at decision point 616. If not OK (NK) then flow returns to entry point "1" in Fig. 6a.

If the result of test 616 is an "OK" response, then flow proceeds to block 617 to store the "dealer OK" result, after which flow returns to entry point "1". The user response of OK or not OK (NK) is conveniently entered with the OK key 5 and the NK key 6, as previously described with respect to Fig. 1.

Continuing in Fig. 6b, if the decision at 613 determines the message is not a dealer's signature, then the message is tested at 618 to see if the received message is a debit message, and if not (no) then flow proceeds to other processing at 619 and entry point "4" leading to Fig. 6c. However, if the test at 618 determines that the message is a debit message (yes), then flow proceeds to block 620 where the amount to be debited from the SmartCard is shown on the terminal display 2, and a user response is awaited, i.e., an OK/NK key press as tested at 621. If the user presses the NK key indicating the debit amount is not correct, then a response is sent to the PC at block 622, and flow returns to entry point "1". However, if the user response is "OK", then flow proceeds to block 623 where the debit message is sent to the SmartCard so that the displayed debit amount will be debited from the SmartCard. A response from the SmartCard is awaited, after which the response from the SmartCard is sent to the PC at block 624, and flow proceeds back to entry point "1".

If the message was not a dealer signature or a debit message, as determined in tests 613 and 618 in Fig. 6b, then flow has proceeded to entry point "4" in Fig. 6c. In this figure, a test is made to determine if the message is a message to be signed

at block 625, and if not, flow proceeds to entry point "1" in Fig. 6a. However, if the message is to be signed, then flow proceeds to block 626 where the message is displayed on the terminal display and a response from the user is awaited. The response is tested at 627, and if it is a not OK, then flow proceeds to block 628 to send the response to the personal computer and return to entry point "1" in Fig. 6a. However, if the response is OK, the flow proceeds to block 629 to sign the message and have it sent to the personal computer. Afterwards, flow returns to entry point "1" in Fig. 6a. During the time the message is being displayed, the user can operate page-up and page-down keys where the message is larger than can be displayed at once on the terminal display, however, the associated process flow has been omitted from the diagrams for the sake of simplicity.

Flow for a credit operation (not shown), i.e., where an amount is to be added to a SmartCard, would be substantially similar to flow for a debit from the SmartCard, the user being shown the amount on the terminal display and a response awaited before either applying the credit or rejecting it and notifying the PC.

It will be apparent to one skilled in the art that the manner of making and using the claimed invention has been adequately disclosed in the above-written description of the preferred embodiment(s) taken together with the drawings.

It will be understood that the above described preferred embodiment(s) of the present invention are susceptible to various modifications, changes, and adaptations, and the same are intended to be comprehended within the meaning and range of equivalents of the appended claims.

Further, although a number of equivalent components may have been mentioned herein which could be used in place of the components illustrated and described with reference to the preferred embodiment(s), this is not meant to be an exhaustive treatment of all the possible equivalents, nor to limit the invention defined by the claims to any particular equivalent or combination thereof. A person skilled in the art would realize that there may be other equivalent components presently known, or to be developed, which could be used within the spirit and scope of the invention defined by the claims.

What is claimed is:

1. A terminal device for use at home in conjunction with a personal computer to facilitate electronic transactions, comprising:

a housing;

a plurality of user-actuable keys, including numeric keys and at least one function key, disposed at a surface of the housing;

a display disposed at a surface of the housing;

a first processor disposed in the housing, operatively coupled to the display and the plurality of keys;

data/program memory disposed in the housing, coupled to the first processor;

at least one interface disposed in the housing, which couples the first processor to a personal computer and to at least one additional external device, and which facilitates an exchange of data between the first processor, the personal computer, and the at least one additional external device; and

a second processor disposed in the housing, the second processor coupled to the first processor, the second processor performing digital signature processing.

2. The terminal device according to claim 1, wherein the at least one interface disposed in the housing, which couples the first processor to at least one additional external device and facilitates an exchange of data between the first processor and the at least one additional external device, comprises an electronic card interface which interfaces the first processor with an electronic card.

3. The terminal device according to claim 1, wherein the at least one interface disposed in the housing, which couples the first processor to at least one additional external device and facilitates an exchange of data between the first processor and the at least one additional external device, comprises a memory card interface which interfaces the first processor with a memory card.

4. The terminal device according to claim 1, wherein the at least one interface disposed in the housing, which couples the first processor to at least one additional external device and facilitates an exchange of data between the first processor and the at least one additional external device, comprises a smart diskette interface which interfaces the first processor with a smart diskette device.

5. The terminal device according to claim 4, wherein the smart diskette interface comprises a connector cable.

6. The terminal device according to claim 4, wherein the smart diskette interface comprises a wireless transceiver.

7. The terminal device according to claim 6, wherein the wireless transceiver uses electromagnetic waves encoded with information comprising one of:

infra-red light waves;

radio frequency waves; or

microwaves.

8. The terminal device according to claim 1, wherein the at least one interface disposed in the housing, which couples the first processor to at least one additional external device and facilitates an exchange of data between the first processor and the at least one additional external device, comprises:

an electronic card interface which interfaces the first processor with an electronic card;

a memory card interface which interfaces the first processor with a memory card; and

a smart diskette interface which interfaces the first processor with a smart diskette device.

9. The terminal device according to claim 1, wherein the at least one interface disposed in the housing, which couples the first processor to the personal computer and to at least one additional external device and facilitates an exchange of data between the first processor, the personal computer, and the at least one additional external device, comprises at least one of:

an electronic card interface;

a memory card interface;

a smart diskette interface;

a serial bus interface;

a parallel bus interface;

a keyboard interface;

a magnetic integrated circuit interface;

a mouse device interface;

a USB interface; and

a PCMCIA interface.

10. The terminal device according to claim 1, further comprising memory storing key information.

11. The terminal device according to claim 1, wherein the first processor is operational to perform at least one of the following interactive functions:

personal identification number processing;

crediting cash value to an electronic card; and

debiting cash value from an electronic card;

and wherein the second processor is operational to process certificates of authenticity and digital signatures.

12. The terminal device according to claim 1, wherein protected functions of the terminal device, including communication with the terminal device display and keypad are hard-coded in a display driver and key pad driver, respectively.

13. A method of electronic commerce using a personal computer interfaced with a home point of sale terminal device, the method comprising utilizing the terminal device according to claim 1.

14. A method of electronic commerce using a personal computer interfaced with a home point of sale terminal device, the method comprising:

establishing a connection between the personal computer and a remote computer over a communications medium;

receiving with the personal computer from the remote computer transaction information which may or may not include a digital signature with a certificate of authenticity;

if the transaction information includes a digital signature with a certificate of authenticity, then transferring the digital signature and certificate of authenticity to the home point of sale terminal from the personal computer and decrypting the certificate of authenticity and digital signature in the home point of sale terminal and displaying the identity of the originator of the digital signature and certificate of authenticity.

15. The method of claim 14, wherein the communications medium comprises the Internet, and wherein the remote computer comprises a web site on the world wide web.

16. The method of claim 14, further comprising:

receiving an OK/not OK input from a user on a keypad of the home point of sale terminal about the displayed identity of the originator of the digital signature and certificate of authenticity.

17. The method of claim 14, further comprising:

displaying a message to be signed and sent from the personal computer to a remote computer on the display of the home point of sale terminal;

receiving an input from a user on a keypad of the home point of sale terminal about the displayed message;

if the input received is an OK input, then signaling the personal computer with the home point of sale terminal to effect signing the message and sending the signed message from the personal computer to the remote computer;

otherwise, if the input received is a not OK input, then signaling the personal computer with the home point of sale terminal to prevent signing of the message or sending of the message from the personal computer to the remote computer.

18. The method of claim 14, further comprising:

displaying an amount to be credited to or debited from a transaction card coupled to the home point of sale terminal, on a display of the home point of sale terminal;

receiving an input from a user on a keypad of the home point of sale terminal about the displayed amount;

if the input received is an OK input, then crediting or debiting the transaction card by the displayed amount;

otherwise, if the input received is a not OK input, then signaling the personal computer with the home point of sale terminal that the amount is not accepted.

19. The method of claim 18, further comprising:

prior to crediting or debiting any amount to or from the transaction card, checking the transaction card and determining whether or not a personal identification number is required;

if a personal identification number is required, then receiving the personal identification number on the keypad of the home point of sale terminal, and checking the personal identification number for authorization.

20. The terminal device according to claim 1, further comprising:

at least one connector cable having a "Y" plug, for coupling to the home point of sale terminal, a mouse or a keyboard of the personal computer, and the personal computer;

wherein a modified keyboard or mouse driver is provided that is operational to provide for communication between the personal computer and the keyboard or the mouse, and further to provide that, when there is a message to the home point of sale terminal from the personal computer or vice versa, then communication is temporarily

set up through the "Y" plug between the home point of sale terminal and the personal computer.

21. The terminal device according to claim 1, wherein the at least one interface disposed in the housing, which couples the first processor to at least one additional external device and facilitates an exchange of data between the first processor and the at least one additional external device, comprises a smart diskette interface which interfaces the first processor with a smart diskette device;

wherein the smart diskette device is adapted to receive a transaction card therein, and includes electronic circuitry for interfacing with a transaction card to establish communication therewith.

22. The terminal device according to claim 21, wherein the smart diskette device is further adapted to receive a removable memory device therein, and includes electronic circuitry for interfacing with a removable memory device to establish communication therewith.

23. The method according to claim 14, wherein a smart diskette device, which can accommodate a transaction card, a removable memory device, or both, is interfaced with the home point of sale terminal device, the method further comprising:

establishing communication between the home point of sale device and the smart diskette device to perform at least one of the following:

reading an electronic cash token amount from the transaction card;

changing an electronic cash token amount of the transaction card;

checking a personal identification number; and

reading/writing data from/to the removable memory device.

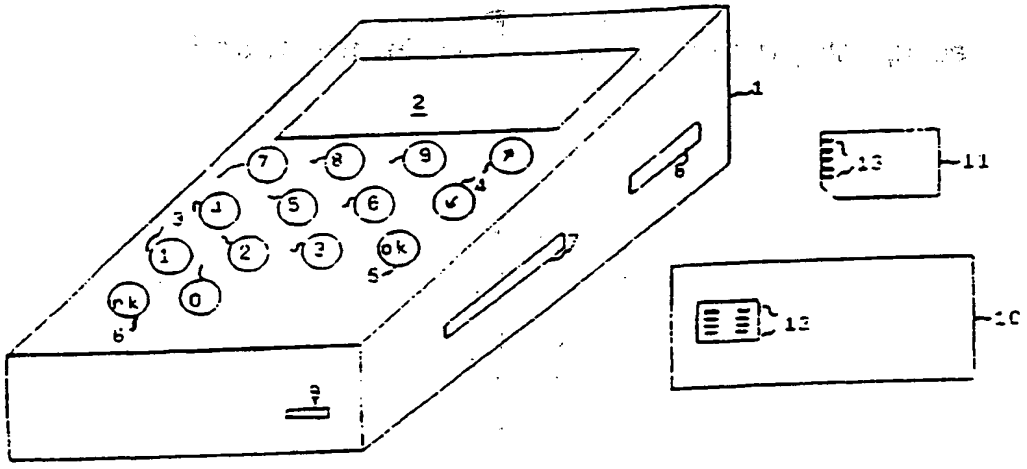

2
1
7
8
9
*
4
3
1
5
6
0
1
2
3
ok
5
ok
6
9
6
13
11
12
10

Fig 1

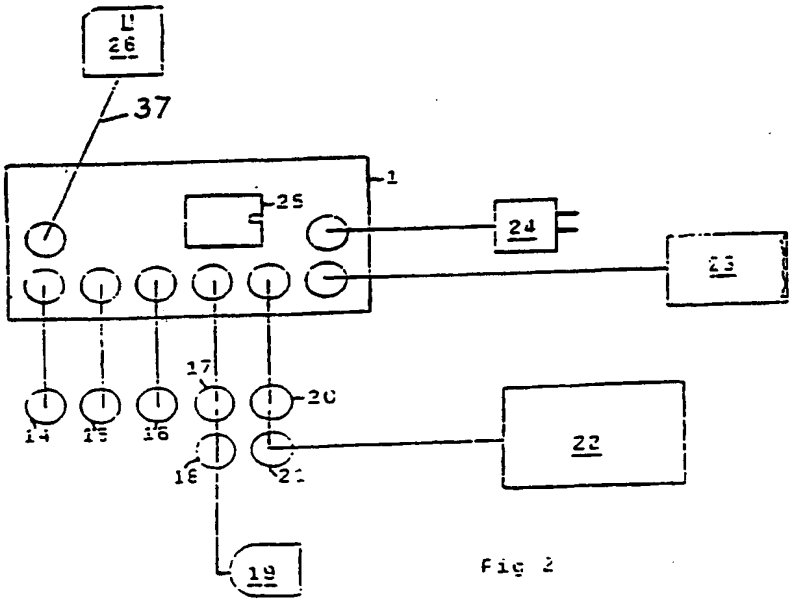

26
37
1
25
24
23
17
20
14
15
16
18
21
22
19

Fig 2

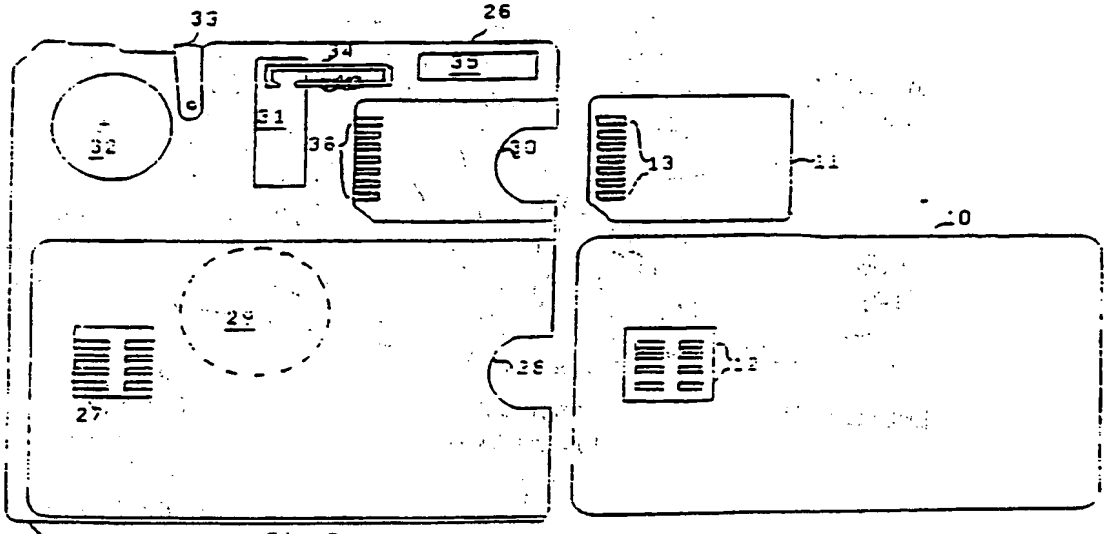


Fig 3

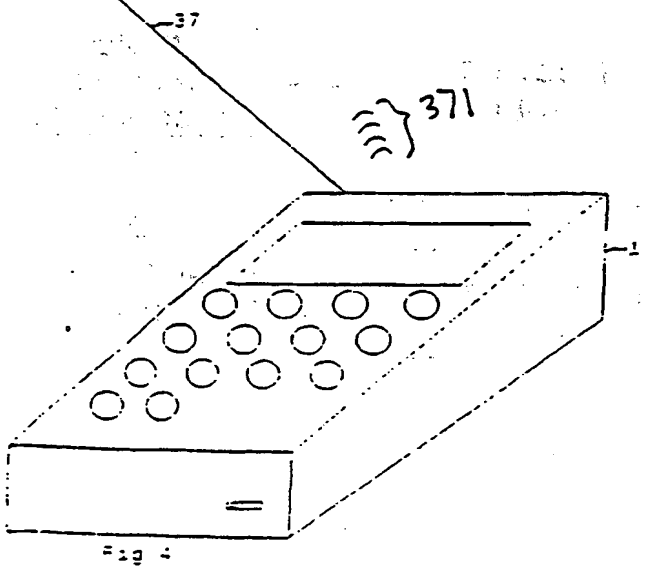


Fig 4

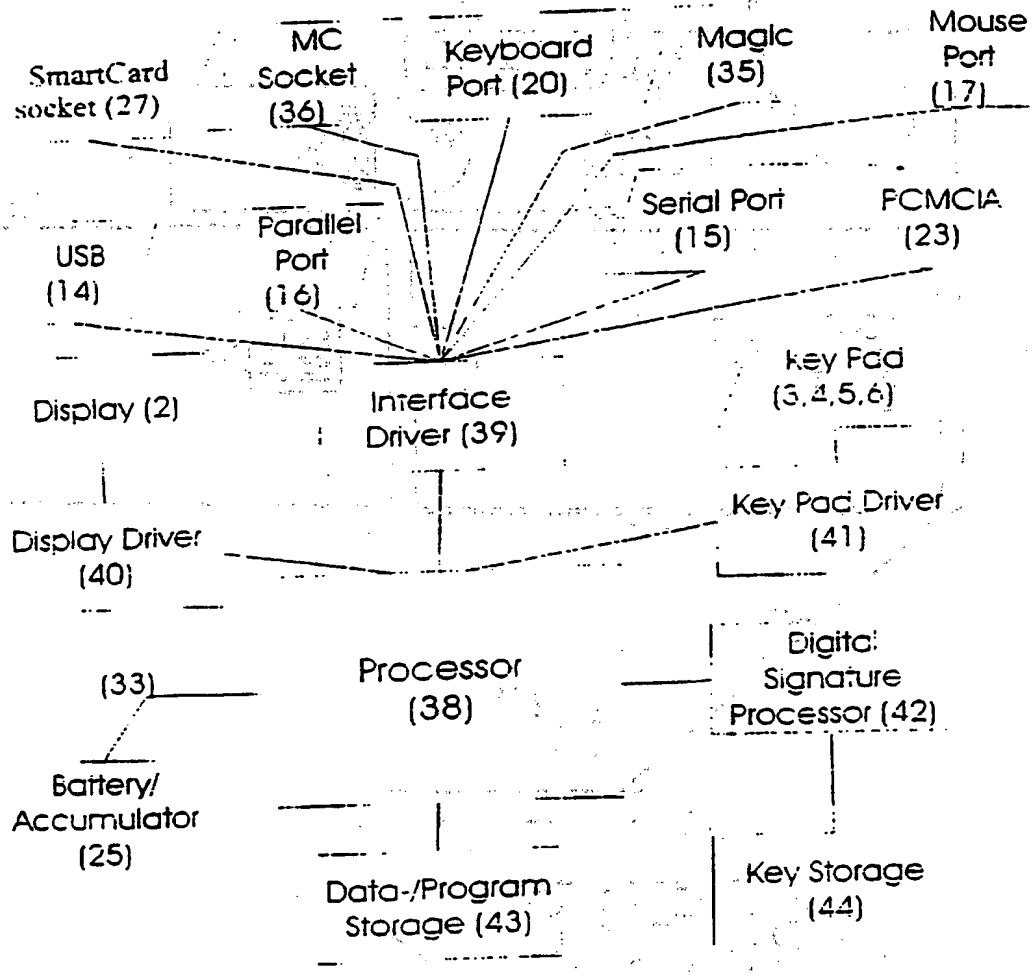

SmartCard socket (27)
MC Socket (36)
Keyboard Port (20)
Magic (35)
Mouse Port (17)
USB (14)
Parallel Port (16)
Serial Port (15)
PCMCIA (23)
Display (2)
Interface Driver (39)
Key Pad (3,4,5,6)
Display Driver (40)
Key Pad Driver (41)
(33)
Processor (38)
Digital Signature Processor (42)
Battery/ Accumulator (25)
Data-/Program Storage (43)
Key Storage (44)

Fig 5

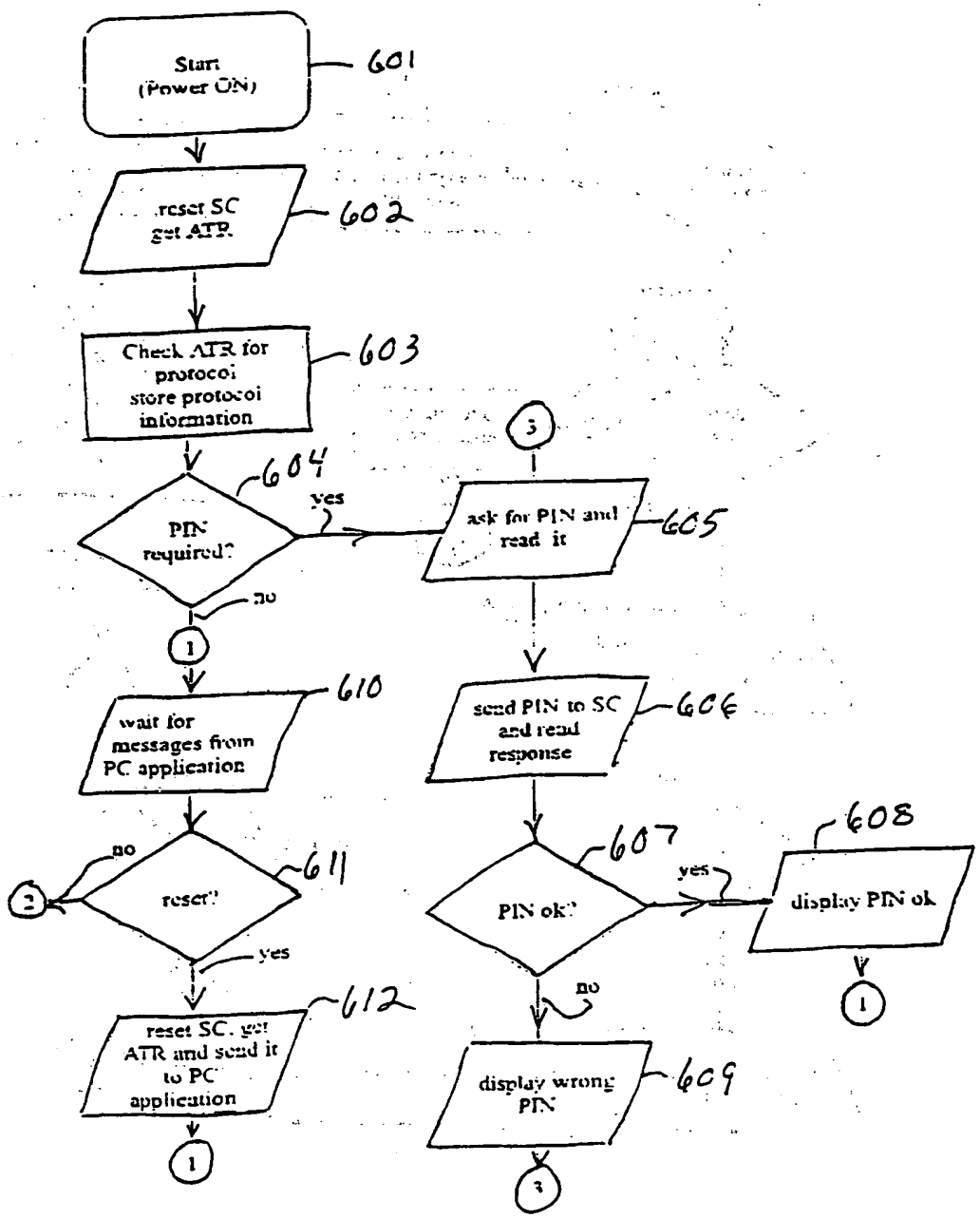

Start
(Power ON)
601
reset SC
get ATR
602
Check ATR for
protocol
store protocol
information
603
PIN
required?
604
yes
no
ask for PIN and
read it
605
send PIN to SC
and read
response
606
PIN ok?
607
yes
no
display PIN ok
608
display wrong
PIN
609
wait for
messages from
PC application
610
reset?
611
no
yes
reset SC, get
ATR and send it
to PC
application
612
1
2
3

Fig 6a

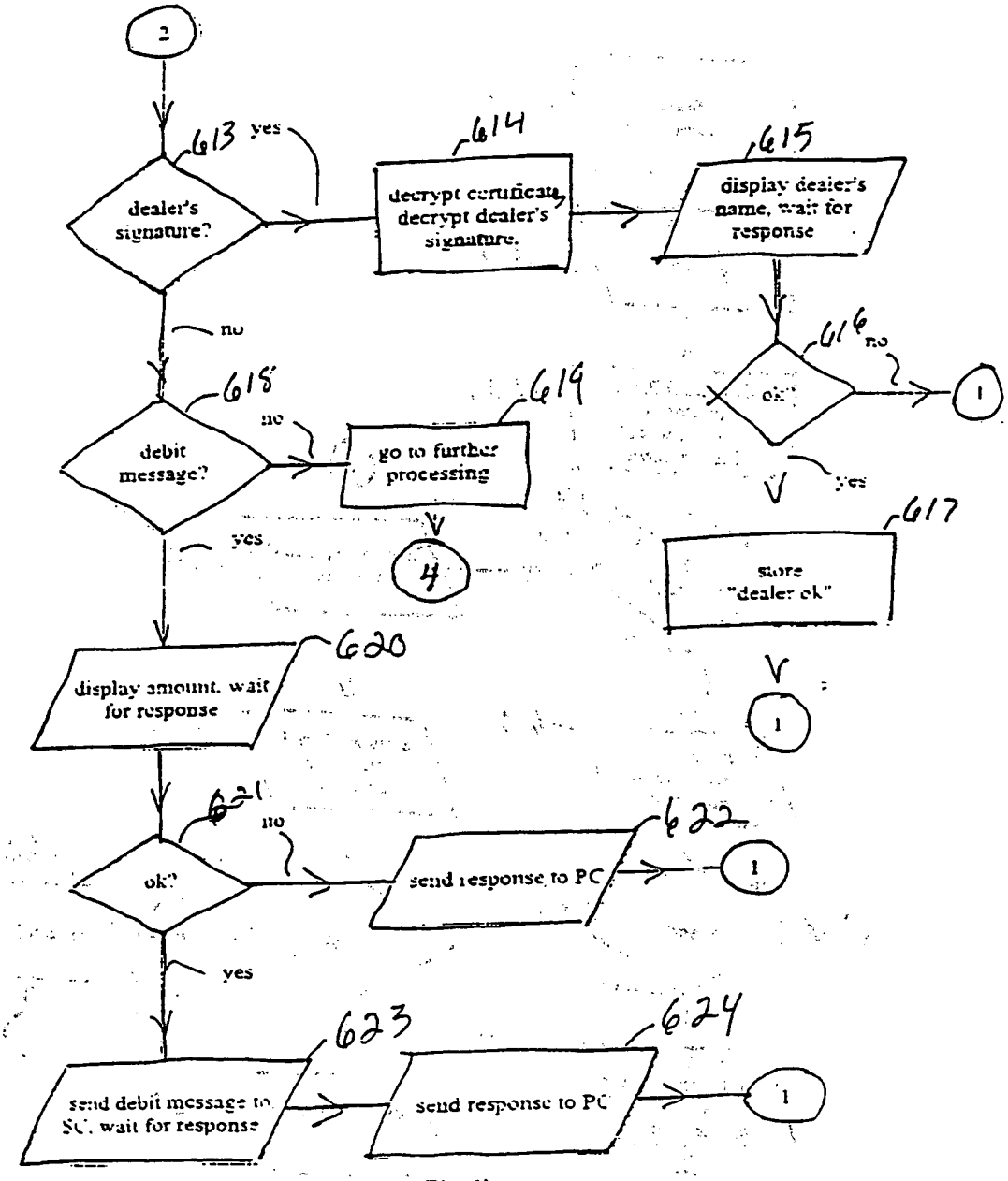

2
613
yes
dealer's signature?
614
decrypt certificate, decrypt dealer's signature.
615
display dealer's name, wait for response
616
no
ok?
1
yes
617
store "dealer ok"
1
no
618
debit message?
no
619
go to further processing
4
yes
620
display amount, wait for response
621
no
ok?
622
send response to PC
1
yes
623
send debit message to SC, wait for response
624
send response to PC
1

Fig 6b

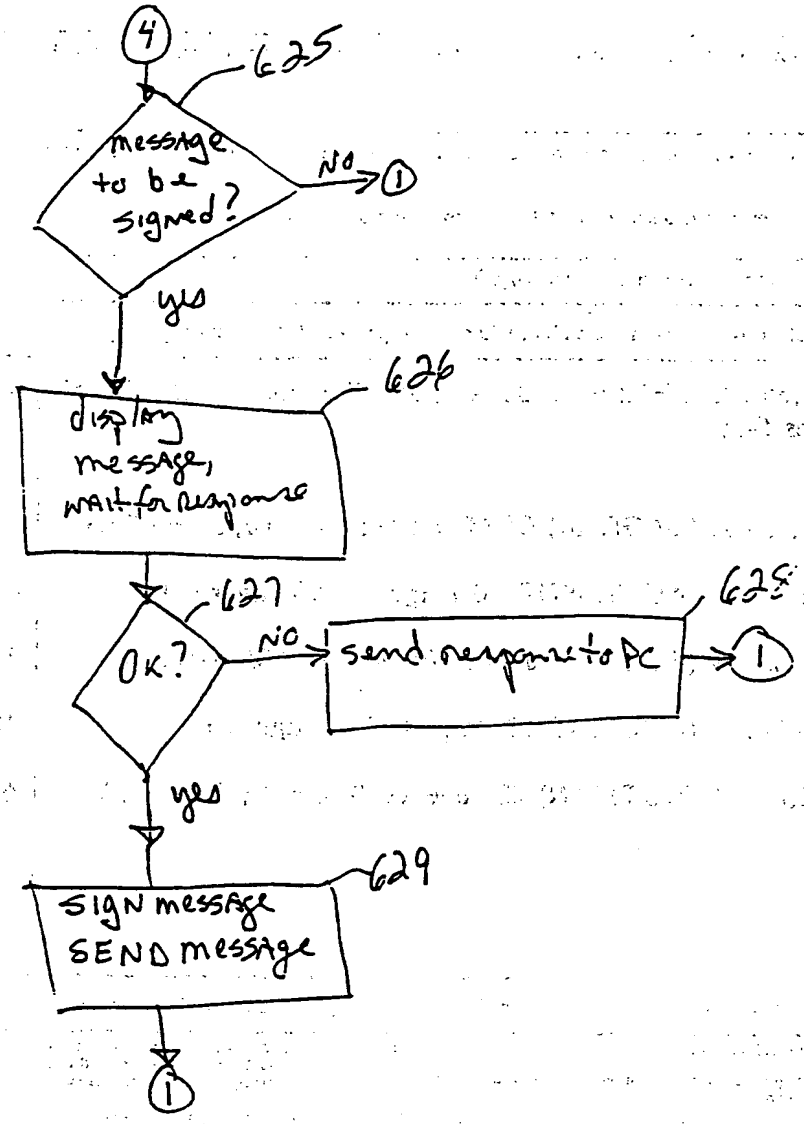

4
625
message to be signed?
NO
1
yes
626
display message, wait for response
627
OK?
NO
send response to PC
625
1
yes
629
SIGN message
SEND message
1

Fig. 6c

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/25584

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :G06F 17/60; G06K 5/00, 19/06, 19/07; HO4L 9/00, 17/02; H04K 1/00
US CL :235/279, 380, 487, 492, 493; 380/23, 24, 25, 49, 52
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 235/279, 380, 487, 492, 493; 380/23 24, 25, 49, 52

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

STN, WEST
search terms: housing, numeric key, display, digital signature, memory card, smart card

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y, P	US 5,945,652 A (OHKI et al) 31 August 1999, col. 7, col. 10; col. 12; figures 6-8;	1-13, 20-22
Y	US 5,748,737 A (DAGGAR) 05 May 1998, col. 10, lines 45-65	1-3, 8-9, 11-13
Y, P	US 5,936,226 A (AUCSMITH) 10 August 1999, figures 1-4	4, 21, 22
Y	US 5,471,038 A (EISELE et al) 28 November 1995, figure 1	5
Y, P	US 5,936,149 A (FISCHER) 10 August 1999, figure 1	10
Y	US 5,221,838 A (GUTMAN) 22 June 1993, col. 2; figures 2B	6, 7

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search
07 JANUARY 2000

Date of mailing of the international search report
10 FEB 2000

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231
Facsimile No. (703) 305-3230

Authorized officer
JAMES P. TRAMMELL
Telephone No. (703) 305-9768

Form PCT/ISA/210 (second sheet)(July 1992) *

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/25584

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,815,577 A (CLARK) 29 September 1998, col. 3; col. 4; col. 5	14-20
Y	US 5,334,823 A (NOBLETT, JR. et al) 02 August 1994, col. 19-22; figures 3-4.	14-19

CORRECTED VERSION*

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
G06F 17/60, G06K 5/00, 19/06, 19/07, H04L 9/00, 17/02, H04K 1/00

A1

(11) International Publication Number: WO 00/26838

(43) International Publication Date: 11 May 2000 (11.05.00)

(21) International Application Number: PCT/US99/25584

(22) International Filing Date: 1 November 1999 (01.11.99)

(30) Priority Data:
09/184,350 2 November 1998 (02.11.98) US

(71) Applicant: SMARTDISK CORPORATION [US/US]; 3506 Mercantile Avenue, Naples, FL 34104-3310 (US).

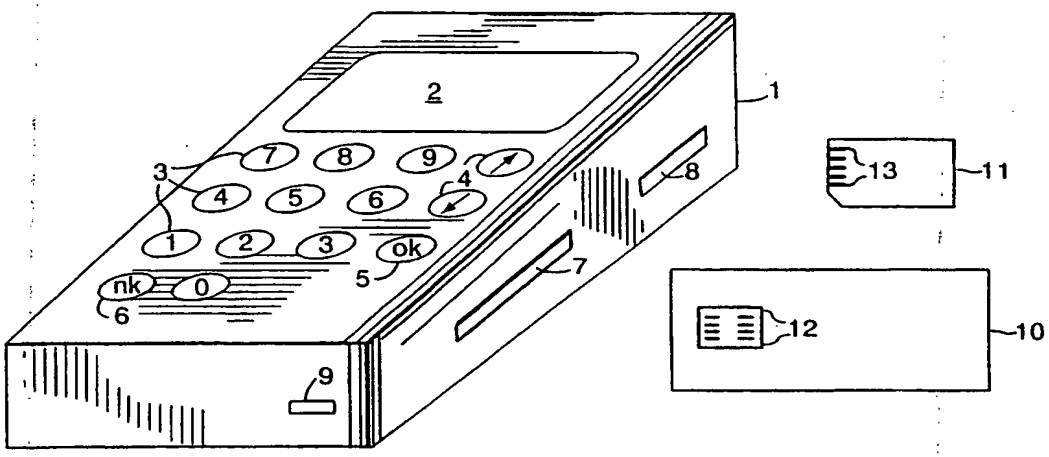
(72) Inventor: EISELE, Raymund; Ferdinand-Abt-Strasse 1, D-65510 Idstein (DE).

(74) Agent: NUSBAUM, Mark, E.; Nixon & Vanderhye P.C., Suite 800, 1100 North Glebe Road, Arlington, VA 22201-4714 (US).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: HOME POINT OF SALE (POS) TERMINAL AND ELECTRONIC COMMERCE METHOD



(57) Abstract

A home point of sale (POS) terminal device provides for enhanced security of electronic commerce transactions.

*(Re-formed to in PCT Gazette No. 45/2000, Section II)

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

HOME POINT OF SALE (POS) TERMINAL AND ELECTRONIC COMMERCE METHOD

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is related to the following application and patent, the subject matter of both being hereby incorporated by reference:

pending application 09/086,677 (Atty Dkt. SMD-0011) filed May 29, 1998, entitled "SMART-CARD AND MEMORY MODULE ADAPTER"; and

U. S. Patent 5,584,043 entitled "APPARATUS HAVING A SMART CARD ACCOMMODATED BY A DISKETTE FRAME CONTAINING PROCESSOR MEMORY AND BATTERY POWER FOR INTERFACING WITH A STANDARD DISKETTE DRIVE."

BACKGROUND OF THE INVENTION

1. Field of The Invention

The present invention relates generally to the field of computer devices, and in particular, to a home point of sale (POS) terminal which is operational to facilitate electronic commerce in conjunction with a personal computer (PC) over the Internet, for example.

2. Background Information

SmartCards and the like are known and have been used for some time in electronic financial transactions, such as making purchases at store-based point-of-sale (POS) terminals, or obtaining cash from automatic teller machines (ATM's). To provide a degree of security, personal identification numbers (PIN's) are generally

required to use such SmartCards. The term SmartCard or "smart-card" as used herein refers to a generally business-card-sized device having a plastic or otherwise semi-rigid/semi-flexible carrier substrate with data storage capability, and which may have processing electronics disposed thereon, such as an ATM card, a patient information card, an electronic cash card, a bank debit card, a FlashPROM card, a credit card, or the like. Sometimes the storage capabilities of such cards are limited to a magnetic strip, while other cards may have several megabytes of electronic memory storage. Such cards are sometimes referred to generically as transaction cards herein. There are also a number of known card communication standards and interfaces to which many cards and associated reading/writing devices adhere. Some cards use electrical contacts while others use magnetic or electrostatic means of communication with associated reading/writing devices. Suffice it to say that there are a variety of cards and devices for reading and/or writing data thereon in usage today.

The variety of transaction cards and associated read/write devices is exemplified by the following publications, the subject matter of which is hereby incorporated by reference. Ishii et al. (5,541,985) disclose a portable electronic device having an external input/output unit and power source integral therewith. An IC card is read from and/or written to with the device which is provided with a control terminal through which power can be turned on/off based on a signal from a portable phone unit. Marceau et al. (5,491,326) disclose a vend card transaction terminal and an associated computer device for implementing inventory and accounting functions. Roberts et al. (5,438,184) disclose a paystation device adapted to be

coupled to a transaction terminal (POS) for carrying out a transaction between a seller and a buyer using a smart card having a cash token value stored therein. Takahashi (5,406,604) discloses an IC card and a portable terminal. Oogita (5,227,615) disclose a portable terminal device having a first interface for a first information exchanging card and a second interface for a second information exchanging card. Johnson et al. (5,149,945) disclose a method a coupler for interfacing a portable data carrier with a host processor, such as a personal computer or point of sale device. Hoppe (5,068,894) discloses a method of generating a unique number for a smart card and its use for the cooperation of the card with a host system. Masuzawa et al. (5,015,830) disclose an electronic card reading device. Hirokawa (4,672,182) disclose a memory card. Dreifus (4,575,621) discloses a portable electronic transaction device and terminal therefore. DE 3528199 discloses a check card system. Oki Electric Industry Co., Ltd. ("OAP Releases Valu-Checker PLUS™ ") announces a personal smart card reader with optional PC Connect adapter to connect to a personal computer through a serial port.

Recently, information exchange and commerce using personal computers, has become increasingly popular, in particular, over the Internet connecting through a network of other computers to a business' World Wide Web (WWW) site. As generally understood by those skilled in the art, the Internet is a global network connecting millions of computers. An internet (lowercase "i") is a network of computers, usually a collection of networks interconnected with routing computers. The Internet (uppercase "I") is the largest internet in the world. It has a three-level

hierarchy composed of backbone networks, mid-level networks, and stub networks. The Internet is a multi-protocol internet using packet-switching between host computers/nodes. Computers on the Internet have an Internet address that uniquely identifies them. The World Wide Web (WWW) is a system of Internet servers that support specially formatted documents, i.e., formatted in a language called HyperText Markup Language (HTML), that supports links to other documents, as well as graphics, audio and video files. There are several application programs called Web browsers which facilitate access to the WWW, e.g., Netscape Navigator and Microsoft's Internet Explorer.

Unfortunately, computer viruses and so-called "Trojan horse" programs can be spread easily and rapidly through this relatively new communications medium, and this presents significant security problems for internet commerce. A computer virus is a program which hides inside another computer program and waits for an opportunity to carry-out its nefarious mission. In general, a Trojan horse program is a program that carries within itself a means to allow the creator of the program access to the system using it. Such a program could, for example, watch for secret information, such as a PIN number entered on a keyboard during an internet credit-card transaction, capture it, and e-mail it to the program's originator for misuse.

Further, when one communicates with a business' Web site, referred to herein as a "virtual shop" on the Internet, there is the question: Is the dealer with which one is communicating really the one which is shown on the personal computer's (PC) display, or an imposter? To be sure of communicating with the correct dealer, encryption and decryption technology has been used to provide a

digital signature of the dealer with a certificate of authenticity from a Certificate Authority. However, a rogue computer program running on the personal computer could deceive a user. In addition, if a users wants to sign a message, there is the question of whether the message being signed is really the message being displayed on the personal computer screen. Again, a rogue program on the personal computer could deceive the user.

Therefore, a need exists for a solution to the security risks and problems caused by rogue programs, such as viruses and Trojan horse programs, in electronic internet commerce.

There is known a so-called "smart-diskette," which is a device having the external shape of a diskette, for example, a standard 3-1/2 inch diskette, and which contains therein, instead of and/or in addition to a magnetic medium (magnetic disk), interface and processing circuitry for providing particular functionality to the device. The circuitry includes an interface for transferring data between other components provided on the device and/or inserted into the device, and a magnetic head of a standard floppy disk drive into which the device can be inserted.

In various forms, the smart-diskette device may include a microprocessor for controlling the device and performing various tasks, such as data encryption and/or compression. On-board memory may be provided as well in the form of, for example, dynamic RAM (random access memory), ROM (read only memory), EEPROM (electronically erasable/programmable read only memory), and/or Flash memory, for storing programs and/or data.

The device circuitry may be provided in the form of discrete components or, advantageously, as a single integrated circuit (IC), in particular, as an application specific integrated circuit (ASIC).

U. S. Patent No. 5,159,182, and copending application S. N. 08/420,796 (Atty Docket No. LWBR 0006C1) hereby incorporated by reference, disclose embodiments of a smart-diskette insertable element with magnetic interface, processor, power supply and optional display and keypad, designed to be inserted into a standard 3-1/2 inch floppy disk drive of a host computer, i.e., electronic data processing (EDP) equipment, such as a desk-top personal computer (PC) or notebook computer, for example.

An exemplary embodiment of the smart-diskette insertable element disclosed in the above-mentioned patent and application, has a processor with some built-in program/data memory. additional memory for storing data and/or programs, and an interface designed to facilitate the exchange of data between the device and a floppy disk drive read/write head. A driver and coil of the interface convert signals from the processor into the required magnetic form and provide them to the read/write head of a floppy disk drive, and likewise convert signals received from the floppy disk drive read/write head into the required form for use by the processor.

An advantage of the smart-diskette insertable element is that, by virtue of its insertability into the standard and ubiquitous (Bill: i.e., universal, omnipresent, prevalent, extremely common, pervasive, found everywhere, proliferated) floppy disk drive of a personal computer, and its interfaceability therewith, it is possible to carry-out a wide variety of operations with the processor and/or memory on the element,

and interactively with the personal computer. These include but are not limited to encryption and decryption of data and/or verification of user identity. Such operations are accomplished without requiring any specially designed interface or plug-in boards which might be suitable only for use with a limited number of computer systems.

Another advantageous feature of the smart-diskette insertable element is its ability to store additional data and/or programs in on-board and/or add-on memory connected with the on-board processor. This considerably increases the potential areas of application for the element.

The smart-diskette element disclosed in the above patent and application may be equipped with a battery power source supplying power to the electronic components within the element, and/or a generator/alternator, with associated regulator circuitry, driven by the rotation of a floppy disk drive spindle.

As mentioned, the interface of the smart-diskette insertable element is designed to allow data to be exchanged with the read/write head of a floppy disk drive. One way this can be achieved is by locating an electromagnetic component on the element, e.g., one or more coils, to be in the vicinity of the read/write head of the floppy disk drive when the element is inserted into the drive, and which generates magnetic field information functionally the same as that generated by a magnetic disk of a standard floppy diskette. In this way, the interface simulates a magnetic floppy diskette. This property of the interface allows data to be transferred under control of the on-board processor to the EDP equipment (e.g., a personal computer), such as data which enables user identification to be verified, thereby

providing security to the EDP equipment, or any of a number of other operations, as would be recognized by one skilled in the art.

As processor capabilities expand and memory devices with increasing capacity become smaller, the smart-diskette device takes on the potential for more and more useful and varied applications.

Related U. S. Patent 5,471,038, hereby incorporated by reference, discloses a special read/write unit with a read/write head and optional electrical contacts, but without the standard disk driving and head moving parts, for use in a desk-top PC or notebook computer to communicate with a smart-diskette. By eliminating the drive motor and moving read/write heads, a significant amount of energy which would otherwise be expended by the use of such moving parts is conserved.

Further, such a read/write unit, since it eliminates bulky drive and head motors, can be made more compact than a standard floppy disk drive, thereby reducing the overall size and weight requirements for the computer in which it is installed.

Related copending application 08/514,382, hereby incorporated by reference, discloses a pocket interface unit (PIU) for use with a smart-diskette. Pocket calculators and diary devices are known and have gained acceptance with busy executives, for example. However, such devices have numerous limitations and disadvantages. For example, although such devices can interface with a desk-top computer to download application programs and/or data, for example, or to upload data entered on the pocket device to the desk-top computer, to do so currently requires inconvenient cabling, and/or a special interface unit, e.g., PCMCIA, with

associated costs. Some devices use infra-red beams to communicate between the device and the PC, but these are subject to atmospheric and distance limitations, or may be subject to errors due to dust or dirt on a lens, for example.

In addition, such pocket devices are generally limited to a single special application, such as a phone directory, or a golf-handicap calculator, and do not generally provide the range of capabilities of a notebook computer, for example. Pocket-sized pagers and cellular telephones are also known. However, these respective devices do not generally have the capability of functioning as anything except a pager or telephone; that is, they are generally devices which are dedicated to a single function. Therefore, the fully-equipped, fully-functional executive may be burdened by having to carry around a variety of separate devices, which further disadvantageously cannot readily interface with one another.

The PIU, disclosed in the copending application, for use with a smart-diskette, overcomes these and other problems, and provides other advantages over existing technology.

Related U. S. Patent 5,584,043, incorporated by reference, discloses a smart-diskette adapted to receive at least one memory and/or processor card, generically referred to herein as a "smart-card," such as an ATM, patient information, electronic cash card, bank debit card, FlashPROM card, credit card, or the like. For example, Figure 5a of that patent illustrates an embodiment adapted for receiving at least one mini-chip card. This patented device can be used with the recently developed MMC (MultiMediaCard made by Siemens/SanDisk), or the SSFDC also called a SmartMediaCard (SMC, made by Toshiba). These compact memory cards are

referred to generically herein as "memory modules" because of their modular configuration.

The so-called MultiMediaCards (MMC's) provide small, transportable audio/video media storage in the form of a modular card substrate carrying a memory, and an optional processor in some cases, which can be inserted into a number of different media recording/playback devices specifically adapted to receive the MMC's. The MMC memory currently can store, for example, about 16 megabytes of digitized video and/or audio signals, however memory capacities are growing almost daily. Typically, contacts on the MMC are be used to connect and transfer the digitized video/audio to a media recorder or playback device.

Although MMC's and the like are a remarkable technological development, until the advent of the smart-diskette embodiment disclosed in the above mentioned patent, which is adapted to receive at least one modular memory card, such as an MMC, a special add-on device would have been required to load data onto an MMC from a personal computer or vice versa. The smart-diskette provides a convenient low-cost alternative to the special add-on device.

A variety of Flash memory devices (e.g., FlashPROM's) have also become known and are more and more widely used, for example, in digital cameras. The above-mentioned SMC's and other memory modules may use Flash memory or any other type of non-volatile memory available.

Further, to use the MMC's as proposed for storing and playing back high-fidelity musical compositions, a user would need an entirely new recording/playback device designed with a port for interconnecting with the MMC's to make use of them

in their home. In other words, the existing conventional user playback/recording equipment, such as an audio cassette player, does not generally interface with the newly developed MMC's. Therefore, a need existed for an adapter device which could permit use of the new MMC's with the existing conventional electronic equipment, such as home/auto recording/playback equipment. Copending application 09/013,036 (Atty Dkt. SMD-0008), hereby incorporated by reference, meets this need and discloses an adapter for use in adapting a conventional cassette tape playback/recording device with a plurality of Flash memory devices, MMC's, or the like, which store digitized audio, for example. The adapter provides a way of adapting one or more MMC's to conventional recording playback devices, such as a conventional audio or video cassette player. The adapter inserted into a conventional tape device interfaces the tape device with one or more removable storage circuits (e.g., MMC's) which store digital audio and/or video data. By accommodating a number of MMC's at once, a user can advantageously record and/or playback an extended audio or visual work with the adapter.

Of course, MMC's, Flash-memory devices, and the like, can be put to other uses besides storing audio and/or video/image data for use in a home or automobile system. They can be used to store any type of digital data imaginable. The inventive adapter disclosed in the copending application is in the form of a tape cassette, i.e., audio, video, or digital (e.g., DAT). While digital tape drives are available as relatively expensive add-on devices for personal computers, these tape drives are not in as widespread use as the floppy disk drives which are provided with practically every personal computer as a standard feature.

To take further advantage of some of the other possibilities of MMC's, Flash-memory devices, and the like, and to overcome problems in the art, an improved adapter element in the shape of a diskette for insertion into a floppy disk drive, which is designed to receive a plurality of memory modules or cards therein, was developed and is disclosed in copending application 09/021,986 (Atty Dkt. SMD-0010), hereby incorporated by reference.

According to an aspect of that disclosed adapter device, up to 5 MMC's can be inserted at once into respective sockets. Two modules are insertable (which also means removable) at the left edge of the adapter, two at the right of the adapter, and one at the rear (outer) edge of the adapter. The adapter with one or more memory modules is insertable into a floppy disk drive front edge (inner edge) first. Further, the adapter provides for playback of music and/or image data, for example, from one or more memory modules, via the floppy disk drive of a personal computer. Music and/or image data, for example, can be recorded on one or more memory modules via the personal computer floppy disk drive.

Further, the inventor realized that there may be times when it would be advantageous to have a single adapter which could accommodate both a smart-card and at least one memory module simultaneously. For example, should a personal computer user wish to purchase a music selection or picture image, for example, over the Internet using their bankcard (smart-card) for payment, they could do so with a smart-diskette adapter described above which interfaces their personal computer with their bankcard. If the user wanted to download the music or image purchased into a memory module, they could do so with another different smart-

diskette adapter, described above, which interfaces their personal computer with an MMC through the floppy drive.

Related co-pending application 09/086,677 (Attorney Docket SMD-0011), provides a method and apparatus for an adapter which can accommodate both a smart-card and at least one memory module at the same time, and thereby provide the functionality of two different adapters in one, as well as a synergistic enhancement of functionality, thereby providing advantages over the prior adapters. This adapter includes a frame having the shape of a diskette, the frame having at least one first recess for receiving an insertable memory module, and a second recess for receiving an insertable smart-card, the frame having therein interface circuitry providing an interface with a read/write head of a floppy disk drive, the memory module, and the smart-card, when inserted in the respective recesses. The frame has the shape and size of a 3-1/2 inch floppy diskette. The at least one first recess is adapted to receive at least one of a plurality of standard memory modules, the plurality of standard memory modules including multi-media cards (e.g., MMC's), and smart media cards (e.g., SMC's or SSFDC's). The interface circuitry includes respective contacts disposed in respective ones of the first and second recesses which couple with corresponding respective contacts on a respective memory module and smart-card when inserted in the respective recesses; a magnetic interface which is adapted to magnetically couple with a read/write head of a floppy disk drive when the adapter is inserted in the floppy disk drive; and a processor, coupled to the contacts, which is operable to receive and transmit signals to and

from the respective memory module and smart-card through the respective contacts, and to receive and transmit signals to and from the magnetic interface.

That adapter further includes a memory connected to the processor which stores data and/or programs used by the processor, and the magnetic interface includes a magnetic transducer which is operable to send and receive magnetic signals to and from a floppy disk drive read/write head, and a driver/converter connected to the transducer and the processor which is operable to convert signals from the transducer to a form useful to the processor, convert signals from the processor to a form used by a floppy disk drive, and to drive the transducer with the converted signals from the processor. At least one battery is provided on the adapter which is connected to provide power to the interface circuitry, at least one memory module, and at least one smart-card. The memory for the processor stores programming enabling the processor to perform at least one of encryption of data, decryption of data, compression of data, and decompression of data. The processor includes programming to perform interactive password checking to verify authorized use of the adapter and/or the at least one memory module and/or the at least one smart-card.

According to that application (09/086,677, Attorney Docket SMD-0011), a method of purchasing data, making payment with a smart-card and storing the data to a memory module, via a terminal having a direct access storage device, e.g., a floppy disk drive, includes utilizing the adapter according to the invention having the smart-card and the memory module inserted therein. The terminal is a personal computer which is connected to the Internet for receiving the data therefrom and

making the payment thereto. Electronically purchasing data is facilitated using the disclosed adapter device which is insertable into a terminal direct access storage device, and which accommodates an electronically readable card and at least one memory module therein. In an exemplary method, an electronically readable card and at least one memory module are inserted in the adapter, and the adapter is inserted into a terminal direct access storage device. Upon selecting with the terminal data to purchase having an associated purchase price, a payment amount corresponding to the purchase price is debited from the electronically readable card, and the data to be purchased is stored in the memory module. The terminal device comprises a personal computer, and the method further includes establishing a communications path between the personal computer and a remote location where the data to be purchased is pre-stored. An anti-piracy mechanism to prevent piracy of copyrighted material is included. Encryption, decryption, compression or decompression on the data to be purchased can be performed before storing the data to the memory module. User identification and user authentication prior to debiting a payment amount from the electronically readable card are provided for as well. The electronically readable card may be an electronic cash card having stored thereon an electronic representation of a cash value, and the debiting includes electronically reducing the stored cash value by the payment amount. The electronically readable card may be a credit card, and the debiting including communicating with the credit card issuer to establish a credit card purchase.

That application (09/086,677, Attorney Docket SMD-0011) further discloses a method of access security using an adapter device which is insertable into a terminal

direct access storage device, and which accommodates an electronically readable card and at least one memory module therein, including pre-storing first user data in a memory module, pre-storing second user data in an electronically readable card, inserting the memory module and the electronically readable card into the adapter, inserting the adapter into a terminal direct access storage device, verifying the user data pre-stored in the memory module and the electronically readable card, and permitting or denying access to the terminal device based on a result of the verifying. The permitting access includes permitting an access level corresponding to the user data.

However, the inventor has recognized that, because of the Trojan Horse type of security issues, for example, a need exists for further improvements in this field to overcome a number of issues related to secure use of SmartCards, especially in internet commerce applications. Some applications require that the SmartCard PIN be entered before communicating with the SmartCard chip. If the PIN is entered via the personal computer's keyboard, then there is the possibility that a Trojan horse program with a keyboard grabber could read the secret PIN.

In order to overcome the problems of ensuring against unauthorized discovery of and misuse of PIN's, as well as other security access information related issues, the present invention provides novel solutions in the form of a Home POS Terminal for smart card use and electronic commerce methods, exemplary embodiments of which are described in detail below.

SUMMARY OF THE INVENTION

It is, therefore, a principle object of this invention to provide a secure method of electronic commerce and an apparatus for implementing a Home POS Terminal.

It is another object of the invention to provide a method and apparatus that solves the above mentioned problems so that electronic commerce can be conducted in a more secure fashion.

These and other objects of the present invention are accomplished by the method and apparatus disclosed herein.

The present invention provides an enhancement of the functionality as is described in the related SmartDiskette patent 5,584,043, and in copending application 09/086,677 (SMD 0011). In addition, the present invention provides advantageous new functions, as will be described below.

As mentioned above, some applications require that a user's SmartCard PIN be entered before permitting communication with the SmartCard chip. However, as mentioned earlier, if the PIN is entered via a personal computer (PC) keyboard, then there is the possibility that a Trojan horse program with a keyboard grabber will read the secret PIN. Therefore, according to an aspect of the invention, it is proposed to provide for the entering of the PIN at the Key Pad of a Home POS Terminal connected to the personal computer, and showing the result of PIN verification at the display of the Home POS Terminal.

According to another aspect of the invention, as mentioned above, when communicating with a virtual shop on the Internet, there is the question of whether the dealer or business with which one is communicating is really the dealer or

business which is shown on the PC's display, or an imposter. To be sure of communicating with the correct dealer or business, one requests a digital signature of the dealer with a certificate of authenticity from a Certificate Authority. According to an aspect of the invention, the certificate and dealer signature are advantageously decrypted in a digital signature processor provided in the Home POS Terminal, and the dealer's real identity is shown on the Home POS Terminal display.

According to another aspect of the invention, when one wants debit a certain amount from, e.g., a stored value on a SmartCard, there is the question of whether the debit amount which is shown on the PC's display is really the amount which will be debited from the SmartCard. According to the invention, the amount that will actually be debited from the SmartCard is displayed on the Home POS Terminal display. The user is able to confirm the amount to be debited, with an "OK." Key on the Home POS Terminal, for example, or to reject the amount, with a not OK key, for example.

According to another aspect of the invention, when a user wants to sign a message to be sent, there is again the question of whether the message shown on the personal computer display is really the one which will be signed, in the SmartCard processor or in the digital signature processor, for example. Therefore, according to an aspect of the invention, the message which will actually be signed will advantageously be displayed on the display of the Home POS Terminal. If it is a long message, for example, which cannot be shown in full on the display of the Home POS Terminal, the user can use page-up/page-down keys advantageously

provided thereon. To confirm the message, the user hits an "OK" key and can thereby be sure that "what you see is what you sign" (wysiwys).

Advantageously, protected functions of the Home POS Terminal, such as communication with the Home POS Terminal display and keypad can be "hard coded" in a display driver and key pad driver, respectively. Other functions, such as for an interface driver, can be down-loaded from the personal computer to the Home POS Terminal.

Advantageously, according to another aspect of the invention, there are provided multiple interfaces to connect a Home POS Terminal to a personal computer (PC). Such interfaces may include parallel and serial interfaces, PCMCIA, USB, mouse and keyboard interfaces.

Connector cables with "Y" plugs, for example for the mouse or keyboard of the personal computer, can be used if there are no other connections available. According to an aspect of the invention, a modified keyboard or mouse driver is installed. Usually, such drivers provide for communication between the personal computer and the keyboard or the mouse. However, with the modified drivers, when there is a message to the Home POS Terminal, then according to the invention, communication will be temporarily switched to be set up through the "Y" plug to the Home POS Terminal.

These and other objects of the present invention are accomplished by the method and apparatus disclosed herein.

BRIEF DESCRIPTION OF THE DRAWINGS

The above and other features and advantages of the invention will become apparent from the following detailed description taken with the drawings in which:

Fig. 1 illustrates a Home POS Terminal according to an exemplary embodiment of the invention.

Fig. 2 illustrates the Home POS Terminal according to Fig. 1, as seen from the back.

Fig. 3 illustrates a SmartDisk (SmartDiskette) with insertable SmartCard and MemoryCard.

Fig. 4 shows an alternative embodiment of the Home POS Terminal with connection to the SmartDisk of Fig. 3.

Fig. 5 is a block diagram of the functional component provided in a Home POS Terminal according to an exemplary embodiment of the invention.

Figs. 6a, 6b, and 6c depict a flow chart illustrating the operation of an exemplary embodiment of a Home POS Terminal according to the invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT(S)

The invention will now be described in more detail by example with reference to the embodiment(s) shown in the Figures. It should be kept in mind that the following described embodiment(s) is only presented by way of example and should not be construed as limiting the inventive concept to any particular physical configuration.

Referring to Fig. 1, shown is a Home POS Terminal according to an exemplary embodiment of the invention. The housing 1 of the Home POS Terminal is shown having a generally rectangular shape, however, the invention is not limited to a rectangular housing but can be any shape able to accommodate the constituent components. Mounted at an upper surface of the housing 1 for easy observation is a display 2 which may be any suitable type, for example, a liquid crystal display (LCD) or a plasma-type display, having one or several columns and rows of display elements for displaying alpha-numeric characters, and symbols, or the like. A group of numerical keys 3 is also provided on the upper surface of the housing as shown. Numerical keys 3 include the numbers 0 through 9 as is apparent. Additional keys may also be provided, in particular, page-up and page-down keys 4, an "OK" key 5, and a not OK "NK" key 6, in order to facilitate easy operation of the terminal.

As will be described in more detail later, the page-down and page-up keys 4 are useful for reading messages to be signed, for example, which have more characters than can be displayed at one time on display 2. The functions of the OK key 5 and the NK (not ok) key 6 are to indicate acceptance (OK) or non-acceptance (NK) of a displayed message/operation/quantity, such as a debit amount, for example, during operation.

A slot 7 for a smart-card is provided on a side of the housing as illustrated, for example, or in any other convenient location, and, of course, a smart-card socket or other means (not shown) is disposed within the slot 7 for establishing a communication path between internal circuitry of the Home POS Terminal and a smart-card when inserted therein. While such a means would typically be a number

of mechanical contacts which mate with corresponding contacts on a smart-card to establish an electrical coupling, other types of coupling are possible, e.g., optical, electro-static, or magnetic-based coupling. For the purposes of this disclosure, mechanical contacts are illustrated, but the invention is not limited to such a configuration, and any number of equivalent structures/means for establishing a communication path between the terminal and an inserted card are possible within the spirit and scope of the invention, as would be apparent to one skilled in the art.

Similarly, a slot 8 for a memory card is also provided disposed, for example, on the same side of the housing as the smart-card slot 7, and having a memory card socket or other means (not shown) disposed within the slot 8 for establishing a communication path between internal circuitry of the Home POS Terminal and a memory-card 11 when inserted therein. As with a smart-card mentioned above, a memory-card could be coupled in any number of ways within the scope and spirit of the invention.

A power on/off switch 9 is shown on a front face of the housing 1 of the Home POS Terminal. Power for the Home POS Terminal could be derived from internal batteries, or from an external power supply, for example. As can be imagined, photo-voltaic cells (not shown) could be provided on the top surface of the housing for charging internal batteries, as are often used with pocket calculators, and other compact electronic devices, for example.

At the right-side of Fig. 1, adjacent to the smart-card slot 7, is shown a representation of a typical smart-card 10. Adjacent to memory-card slot 8 is shown a representation of a typical memory card 11. The smart-card 10 is shown having

smart-card contacts 12, while the memory-card 11 is shown having memory-card contacts 13, as examples of ways to establish communication with the terminal. The smart-card 10 and memory-card 11 are shown in schematic form and, as is known in the art, may have any number of shapes and sizes or configurations. A number of these have become "standard" as would be appreciated by one skilled in the art., and the Home POS Terminal would be designed and built to accommodate one or more of these "standard" configurations.

Fig. 2 is a drawing of an exemplary embodiment of a Home POS Terminal, such as is shown in Fig. 1, as seen from the back. The Home POS Terminal housing 1 is advantageously provided with a number of different interface connectors, examples of which include a connector 14 for a USB (Universal Serial Bus) interface, a connector 15 for a Serial Port (e.g., RS-232), a connector 16 for a Parallel Bus Port (e.g., PCI), a connector 17 for a Mouse Port with a "Y" plug cable to connect to a Mouse cable of a personal computer (not shown), reference numeral 18 being the Y-connector portion leading to the Mouse 19, a connector 20 for a Keyboard 22 of a personal computer with a "Y" plug cable to connect to a Keyboard cable, reference numeral 21 representing the Y-connector portion leading to the Keyboard 22, and a connector 23 for a PCMCIA card. The Mouse Port "Y" plug cable, and likewise the Keyboard "Y" plug cable, would be configured to be switchable, under control of modified drivers, between communication with the mouse (Keyboard) and with the Home POS Terminal, as is within the skill of one well-versed in the art. A connection for an optional battery Power Charger 24 is also conveniently provided for at the back of the housing 1, for charging a Battery 25

which powers the circuitry (described later) in the Home POS Terminal housing 1. Of course, other types of power supply configurations are possible, as would be apparent to one skilled in the art.

A connection line (37) leading to a SmartDiskette 26 (also referred to as a SmartDisk herein), such as has been described in the Background section above, is also shown in Fig. 2 and will be described in more detail with reference to Figs. 3 and 4. In particular, Fig. 3: illustrates a representative SmartDiskette 26 which can accommodate an insertable SmartCard 10 and/or MemoryCard 11, and Fig. 4 shows the Home POS Terminal connected thereto. In this alternative embodiment of the terminal, slots for the SmartCard 10 and MemoryCard 11 are provided in the SmartDisk 26 rather than, or in addition to, being provided in the terminal housing 1. As should be apparent, the SmartDisk 26 might be configured differently such that it only accommodates the SmartCard 10, or a MemoryCard (or MemoryCards) 11.

The SmartCard 10 and the MemoryCard 11 shown in Fig. 3 have SmartCard contacts 12 and MemoryCard contacts 13 respectively, which mate with corresponding contact sockets 27 and 36 in the SmartDisk 26. A SmartCard recess 28 is provided for aiding insertion and removal of the SmartCard 10. A MemoryCard recess 30 is likewise provided for aiding insertion and removal of the MemoryCard 11. The SmartDisk 26 has a spindle recess 29 for accommodating a disk drive spindle when the SmartDisk 26 is itself inserted into such a drive. Likewise provided is a slot 31 for the read/write head of such a drive. The SmartDisk 26 may have an optional battery 32 and a power on/off switch 33 which is designed to turn on power

to the SmartDisk circuitry when it is inserted into a disk drive, and turn off power when it is removed from the disk drive.

A transducer 34 is shown adjacent to the slot 31 for receiving and sending magnetic signals with the head of a disk drive. A "MagIC" (Magnetic Interface Chip) 35 is likewise provided which is, for example, an Application Specific Interface Chip (ASIC) custom designed to provide the SmartDisk interface functions. Such a SmartDisk 26 is the subject of the related copending applications mentioned and incorporated herein, and a detailed description thereof is not necessary here for a complete understanding of the invention.

Fig. 4. Shows an embodiment of the Home POS Terminal with a connection 37 to the SmartDisk 26 of Fig. 3. In this illustrated embodiment of the Home POS Terminal, the SmartCard and MemoryCard interfaces are not provided in the terminal housing 1, but are provided instead in the SmartDisk 26. The connector cable 37 between Home POS Terminal housing 1 and the SmartDisk 26 may contain, for example, connections to the socket 27 for the SmartCard contacts 12, the MagIC (Magnetic Interface Chip) 35, the socket 36 for the MemoryCard contacts 13, and the power on/off switch 33. However, instead of a cable 37, the connection could also be established via free-space transmission of information encoded infrared light or radio frequency waves (e.g., microwaves), for example, as indicated by lines 371. Of course in that case, the Home POS Terminal housing 1 and the SmartDisk 26 would be provided with respective free-space transceiver circuitry, as would be apparent to one skilled in the art.

Fig. 5 illustrates a block diagram of exemplary components which would be disposed inside the housing 1 of a Home POS Terminal made according to an embodiment of the invention. This figure also shows schematically the functional connections between the different components. Some of the components illustrated here have already been described in detail with respect to the previous figures, and may only briefly be mentioned again. An interface driver 39 is provided which drives the USB 14, the parallel port 16, the serial port 15, the PCMCIA interface 23, the SmartCard socket 27, the MemoryCard (MC) socket 36, the Keyboard port 20, the MagIC interface 35, and the mouse port 17, as illustrated by the lines connecting these to the interface driver 39. Of course, the block labeled interface driver 39 could be implemented by a single special purpose integrated circuit, a number of integrated circuits, or a combination of discrete interface logic circuits, for example. It should be apparent that the interface driver block 39 could alternatively represent a program module of a microprocessor or microcontroller, for example.

A display driver 40 for display 2, and a keypad driver for the keypad keys 3, 4, 5, 6, are likewise provided, and may be implemented in any of the above described ways. The Interface driver 39, the display driver 40 and the keypad driver 41 provide a connection to the main processor 38, which controls the overall operation of the Home POS Terminal. Power is provided by battery 25, for example, and the SmartDisk switch 33 (see Fig. 3) may be bypassed to provide power to a SmartDisk 26 as indicated by "(33)" at the line between the battery 25 and the processor 38. As described, the switch 33 is configured to power the SmartDisk when it is inserted

in a ubiquitous floppy drive, so in the Fig. 3/4 embodiment, it is bypassed by the signal/connection (33) of Fig. 5.

Associated data and/or program storage 43 is provided in the form of RAM/ROM or other memory, coupled to the processor 38. A digital signature processor 42 is also provided for processing digital signatures, as is understood in the art. Key storage 44 is associated with the digital signature processor 42, as shown. The digital signature processor 42 operates to process digital signatures and certificates in order to verify the authenticity and origination of messages, for example, displaying the result on display 2 by way of the processor 38 and the display driver 40. As is known in the art, digital signal processors (DSP's), for example, are used for the function of digital signature processing. As mentioned earlier, display and key pad drivers (40, 41) may be advantageously hard-coded in the terminal to prevent their compromise by nefarious programs.

Figs. 6a, 6b, and 6c illustrate a Flow Chart of the operation of an exemplary embodiment of the invention. In particular, the flow chart shows the functional flow involved in reading a customer PIN from PIN Pad 3, PIN verification in SmartCard 10, and display of the result on display 2.

In more detail with reference to Fig. 6a, the routine starts with power on 601. At this point 602, the SmartCard (SC) is reset and the ATR (Answer To Reset) is obtained. Next at block 603, the ATR is then checked for protocol, and the protocol information is stored. Flow then proceeds to the decision point 604 where it is determined whether a PIN is required. If the answer is YES, flow proceeds to block 605, where the PIN is requested and read into the terminal. Next, at block 606, the

PIN is sent to the SmartCard (SC) and a response is read. If the response indicates that the PIN is correct (OK) at decision point 607, then flow proceeds to block 608 to display a PIN "OK" message, after which flow goes to entry point "1". If at decision point 607 it is determined that the PIN is not OK, then flow proceeds to block 609 to display a PIN wrong message, after which flow goes to entry point "3" to ask for the PIN again (605). Of course, although not shown, after a certain number of wrong PIN entries, the device could stop and execute additional security routines under the assumption that a security breach is being attempted.

If no PIN is required at decision point 604, or after the PIN has been correctly entered and flow has gone to entry point "1", then the routine proceeds to block 610 to wait for messages from the personal computer (PC) application and test for a reset message at 611. If no reset message is detected at 611, flow proceeds to entry point "2" in Fig. 6b. However, if a reset message is detected at 611, flow proceeds to block 612 where the SmartCard (SC) is reset, and the ATR is obtained and sent to the PC application, after which flow returns to entry point "1".

Shown in Fig. 6b is the flow of operation if the received message is not a reset, i.e., it is a digital signature of a dealer for example. That is, flow has proceeded from decision point 611 in Fig. 6a to entry point "2". Decision point 613 tests for a dealer's signature at 613, and proceeds to 614 if it has determined there is a dealer's signature. In block 614 the certificate will be decrypted (i.e., in Digital Signature Processor 42) to receive the dealer's public key which is then used to decrypt the dealer's signature, and then in block 615, the result (dealer's name) is displayed on display 2, and a user response is awaited, i.e., either an "OK" or a not

OK "NK", as tested at decision point 616. If not OK (NK) then flow returns to entry point "1" in Fig. 6a.

If the result of test 616 is an "OK" response, then flow proceeds to block 617 to store the "dealer OK" result, after which flow returns to entry point "1". The user response of OK or not OK (NK) is conveniently entered with the OK key 5 and the NK key 6, as previously described with respect to Fig. 1.

Continuing in Fig. 6b, if the decision at 613 determines the message is not a dealer's signature, then the message is tested at 618 to see if the received message is a debit message, and if not (no) then flow proceeds to other processing at 619 and entry point "4" leading to Fig. 6c. However, if the test at 618 determines that the message is a debit message (yes), then flow proceeds to block 620 where the amount to be debited from the SmartCard is shown on the terminal display 2, and a user response is awaited, i.e., an OK/NK key press as tested at 621. If the user presses the NK key indicating the debit amount is not correct, then a response is sent to the PC at block 622, and flow returns to entry point "1". However, if the user response is "OK", then flow proceeds to block 623 where the debit message is sent to the SmartCard so that the displayed debit amount will be debited from the SmartCard. A response from the SmartCard is awaited, after which the response from the SmartCard is sent to the PC at block 624, and flow proceeds back to entry point "1".

If the message was not a dealer signature or a debit message, as determined in tests 613 and 618 in Fig. 6b, then flow has proceeded to entry point "4" in Fig. 6c. In this figure, a test is made to determine if the message is a message to be signed

at block 625, and if not, flow proceeds to entry point "1" in Fig. 6a. However, if the message is to be signed, then flow proceeds to block 626 where the message is displayed on the terminal display and a response from the user is awaited. The response is tested at 627, and if it is a not OK, then flow proceeds to block 628 to send the response to the personal computer and return to entry point "1" in Fig. 6a. However, if the response is OK, the flow proceeds to block 629 to sign the message and have it sent to the personal computer. Afterwards, flow returns to entry point "1" in Fig. 6a. During the time the message is being displayed, the user can operate page-up and page-down keys where the message is larger than can be displayed at once on the terminal display, however, the associated process flow has been omitted from the diagrams for the sake of simplicity.

Flow for a credit operation (not shown), i.e., where an amount is to be added to a SmartCard, would be substantially similar to flow for a debit from the SmartCard, the user being shown the amount on the terminal display and a response awaited before either applying the credit or rejecting it and notifying the PC.

It will be apparent to one skilled in the art that the manner of making and using the claimed invention has been adequately disclosed in the above-written description of the preferred embodiment(s) taken together with the drawings.

It will be understood that the above described preferred embodiment(s) of the present invention are susceptible to various modifications, changes, and adaptations, and the same are intended to be comprehended within the meaning and range of equivalents of the appended claims.

Further, although a number of equivalent components may have been mentioned herein which could be used in place of the components illustrated and described with reference to the preferred embodiment(s), this is not meant to be an exhaustive treatment of all the possible equivalents, nor to limit the invention defined by the claims to any particular equivalent or combination thereof. A person skilled in the art would realize that there may be other equivalent components presently known, or to be developed, which could be used within the spirit and scope of the invention defined by the claims.

What is claimed is:

1. A terminal device for use at home in conjunction with a personal computer to facilitate electronic transactions, comprising:

a housing;

a plurality of user-actuable keys, including numeric keys and at least one function key, disposed at a surface of the housing;

a display disposed at a surface of the housing;

a first processor disposed in the housing, operatively coupled to the display and the plurality of keys;

data/program memory disposed in the housing, coupled to the first processor;

at least one interface disposed in the housing, which couples the first processor to a personal computer and to at least one additional external device, and which facilitates an exchange of data between the first processor, the personal computer, and the at least one additional external device; and

a second processor disposed in the housing, the second processor coupled to the first processor, the second processor performing digital signature processing.

2. The terminal device according to claim 1, wherein the at least one interface disposed in the housing, which couples the first processor to at least one additional external device and facilitates an exchange of data between the first processor and the at least one additional external device, comprises an electronic card interface which interfaces the first processor with an electronic card.

3. The terminal device according to claim 1, wherein the at least one interface disposed in the housing, which couples the first processor to at least one additional external device and facilitates an exchange of data between the first processor and the at least one additional external device, comprises a memory card interface which interfaces the first processor with a memory card.

4. The terminal device according to claim 1, wherein the at least one interface disposed in the housing, which couples the first processor to at least one additional external device and facilitates an exchange of data between the first processor and the at least one additional external device, comprises a smart diskette interface which interfaces the first processor with a smart diskette device.

5. The terminal device according to claim 4, wherein the smart diskette interface comprises a connector cable.

6. The terminal device according to claim 4, wherein the smart diskette interface comprises a wireless transceiver.

7. The terminal device according to claim 6, wherein the wireless transceiver uses electromagnetic waves encoded with information comprising one of:

infra-red light waves;

radio frequency waves; or

microwaves.

8. The terminal device according to claim 1, wherein the at least one interface disposed in the housing, which couples the first processor to at least one additional external device and facilitates an exchange of data between the first processor and the at least one additional external device, comprises:

an electronic card interface which interfaces the first processor with an electronic card;

a memory card interface which interfaces the first processor with a memory card; and

a smart diskette interface which interfaces the first processor with a smart diskette device.

9. The terminal device according to claim 1, wherein the at least one interface disposed in the housing, which couples the first processor to the personal computer and to at least one additional external device and facilitates an exchange of data between the first processor, the personal computer, and the at least one additional external device, comprises at least one of:

an electronic card interface;

a memory card interface;

a smart diskette interface;

a serial bus interface;

a parallel bus interface;

a keyboard interface;

a magnetic integrated circuit interface;

a mouse device interface;

a USB interface; and

a PCMCIA interface.

10. The terminal device according to claim 1, further comprising memory storing key information.

11. The terminal device according to claim 1, wherein the first processor is operational to perform at least one of the following interactive functions:

personal identification number processing;

crediting cash value to an electronic card; and

debiting cash value from an electronic card;

and wherein the second processor is operational to process certificates of authenticity and digital signatures.

12. The terminal device according to claim 1, wherein protected functions of the terminal device, including communication with the terminal device display and keypad are hard-coded in a display driver and key pad driver, respectively.

13. A method of electronic commerce using a personal computer interfaced with a home point of sale terminal device, the method comprising utilizing the terminal device according to claim 1.

14. A method of electronic commerce using a personal computer interfaced with a home point of sale terminal device, the method comprising:

establishing a connection between the personal computer and a remote computer over a communications medium;

receiving with the personal computer from the remote computer transaction information which may or may not include a digital signature with a certificate of authenticity;

if the transaction information includes a digital signature with a certificate of authenticity, then transferring the digital signature and certificate of authenticity to the home point of sale terminal from the personal computer and decrypting the certificate of authenticity and digital signature in the home point of sale terminal and displaying the identity of the originator of the digital signature and certificate of authenticity.

15. The method of claim 14, wherein the communications medium comprises the Internet, and wherein the remote computer comprises a web site on the world wide web.

16. The method of claim 14, further comprising:

receiving an OK/not OK input from a user on a keypad of the home point of sale terminal about the displayed identity of the originator of the digital signature and certificate of authenticity.

17. The method of claim 14, further comprising:

displaying a message to be signed and sent from the personal computer to a remote computer on the display of the home point of sale terminal;

receiving an input from a user on a keypad of the home point of sale terminal about the displayed message;

if the input received is an OK input, then signaling the personal computer with the home point of sale terminal to effect signing the message and sending the signed message from the personal computer to the remote computer;

otherwise, if the input received is a not OK input, then signaling the personal computer with the home point of sale terminal to prevent signing of the message or sending of the message from the personal computer to the remote computer.

18. The method of claim 14, further comprising:

displaying an amount to be credited to or debited from a transaction card coupled to the home point of sale terminal, on a display of the home point of sale terminal;

receiving an input from a user on a keypad of the home point of sale terminal about the displayed amount;

if the input received is an OK input, then crediting or debiting the transaction card by the displayed amount;

otherwise, if the input received is a not OK input, then signaling the personal computer with the home point of sale terminal that the amount is not accepted.

19. The method of claim 18, further comprising:

prior to crediting or debiting any amount to or from the transaction card, checking the transaction card and determining whether or not a personal identification number is required;

if a personal identification number is required, then receiving the personal identification number on the keypad of the home point of sale terminal, and checking the personal identification number for authorization.

20. The terminal device according to claim 1, further comprising:

at least one connector cable having a "Y" plug, for coupling to the home point of sale terminal, a mouse or a keyboard of the personal computer, and the personal computer;

wherein a modified keyboard or mouse driver is provided that is operational to provide for communication between the personal computer and the keyboard or the mouse, and further to provide that, when there is a message to the home point of sale terminal from the personal computer or vice versa, then communication is temporarily

set up through the "Y" plug between the home point of sale terminal and the personal computer.

21. The terminal device according to claim 1, wherein the at least one interface disposed in the housing, which couples the first processor to at least one additional external device and facilitates an exchange of data between the first processor and the at least one additional external device, comprises a smart diskette interface which interfaces the first processor with a smart diskette device;

wherein the smart diskette device is adapted to receive a transaction card therein, and includes electronic circuitry for interfacing with a transaction card to establish communication therewith.

22. The terminal device according to claim 21, wherein the smart diskette device is further adapted to receive a removable memory device therein, and includes electronic circuitry for interfacing with a removable memory device to establish communication therewith.

23. The method according to claim 14, wherein a smart diskette device, which can accommodate a transaction card, a removable memory device, or both, is interfaced with the home point of sale terminal device, the method further comprising:

establishing communication between the home point of sale device and the smart diskette device to perform at least one of the following:

reading an electronic cash token amount from the transaction card;

changing an electronic cash token amount of the transaction card;

checking a personal identification number; and

reading/writing data from/to the removable memory device.

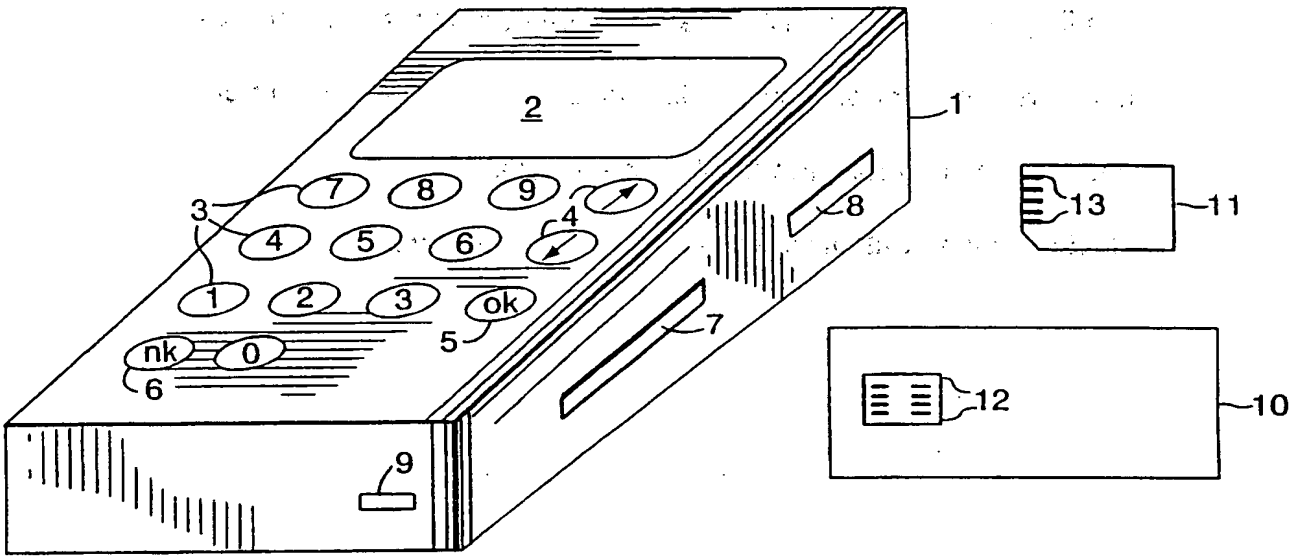

2
1
3
7
8
9
4
4
5
6
8
13
11
1
2
3
ok
5
nk
0
6
7
12
10
9

Fig. 1

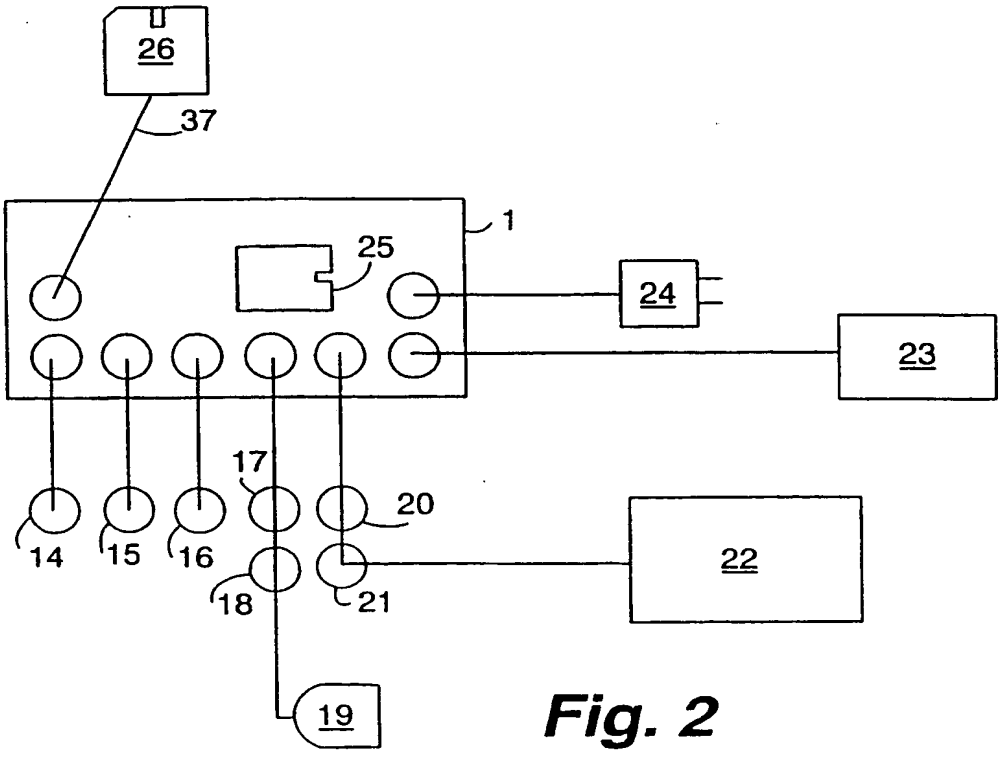
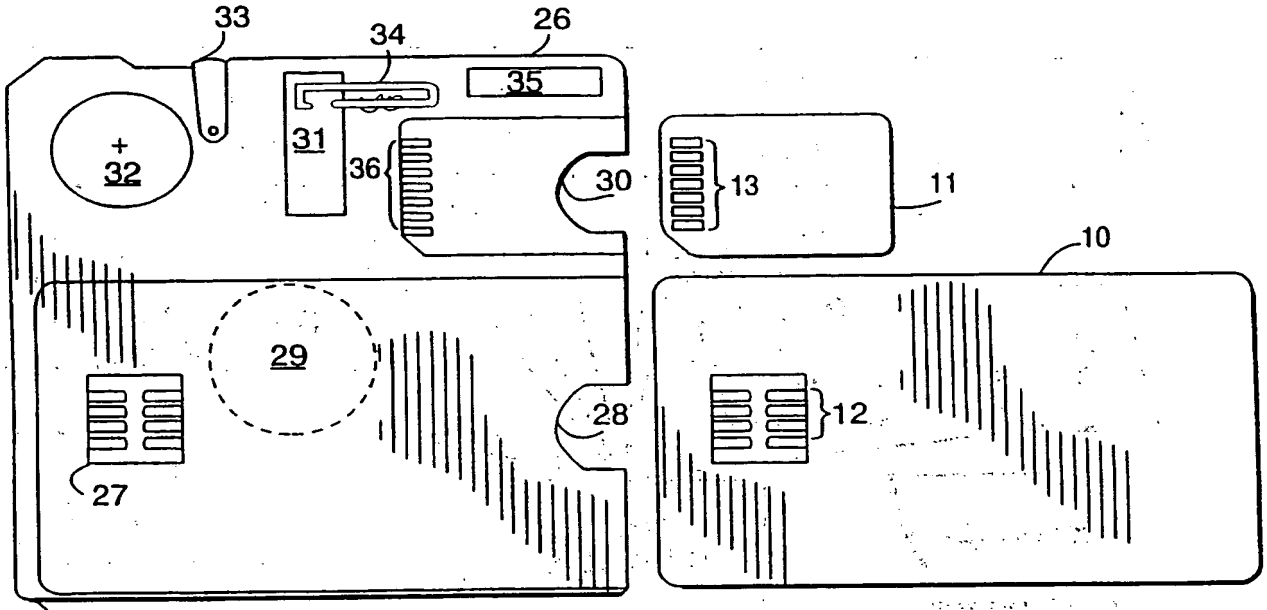

26
37
1
25
24
23
17
20
14
15
16
18
21
22
19

Fig. 2

Fig. 3



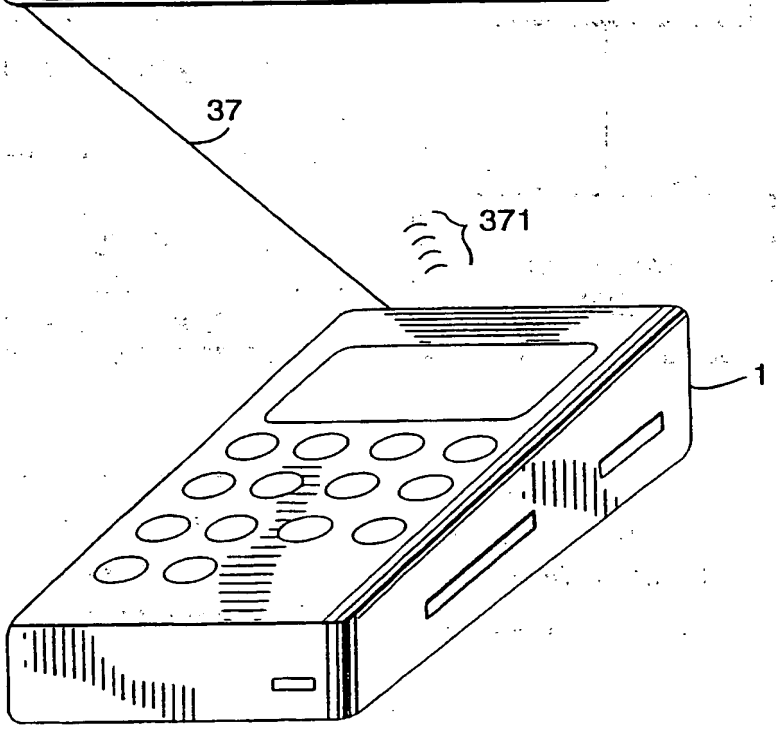
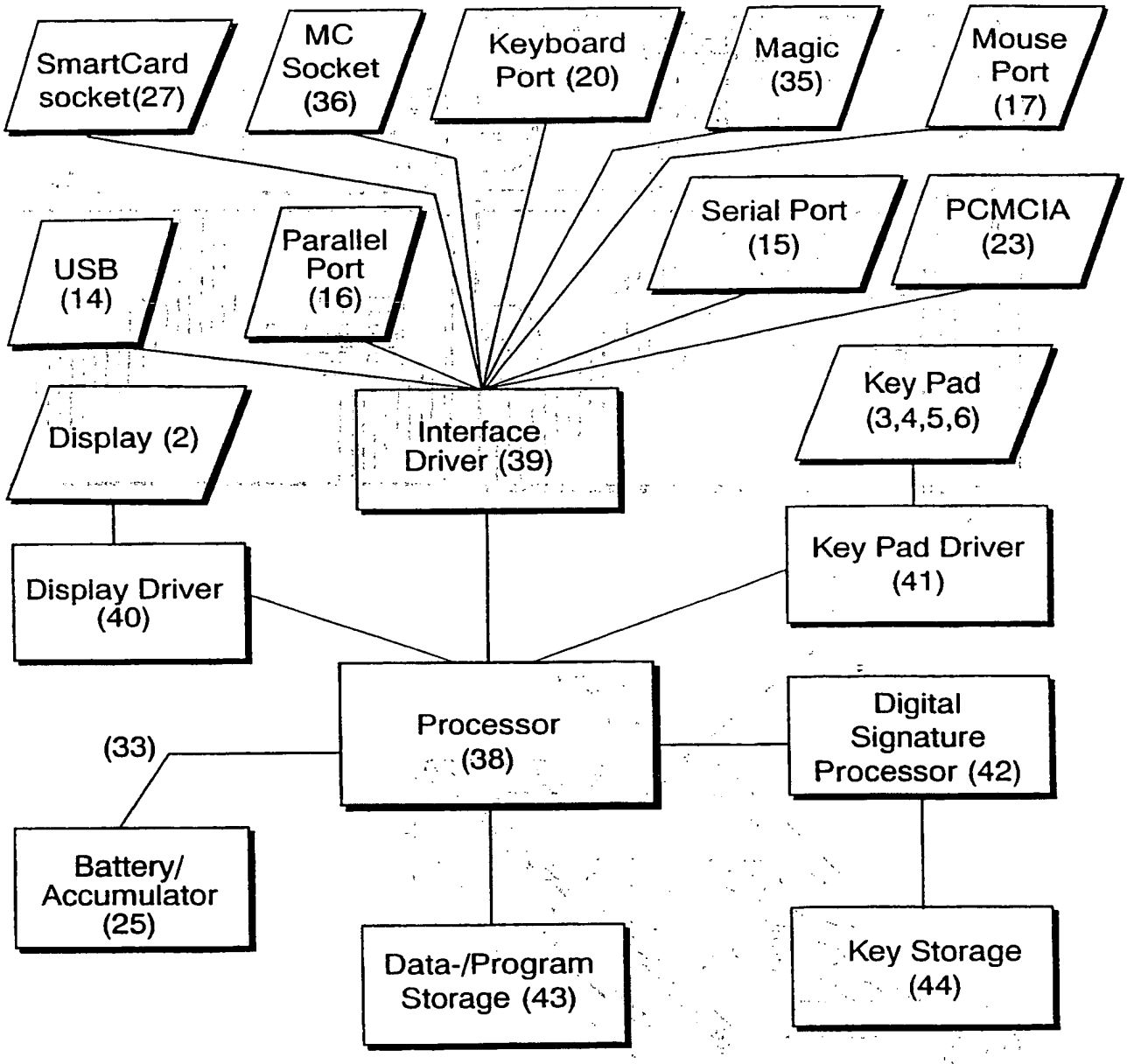


Fig. 4

Fig. 5


SmartCard socket(27)
MC Socket (36)
Keyboard Port (20)
Magic (35)
Mouse Port (17)
USB (14)
Parallel Port (16)
Serial Port (15)
PCMCIA (23)
Display (2)
Interface Driver (39)
Key Pad (3,4,5,6)
Display Driver (40)
Key Pad Driver (41)
Processor (38)
(33)
Digital Signature Processor (42)
Battery/ Accumulator (25)
Data-/Program Storage (43)
Key Storage (44)

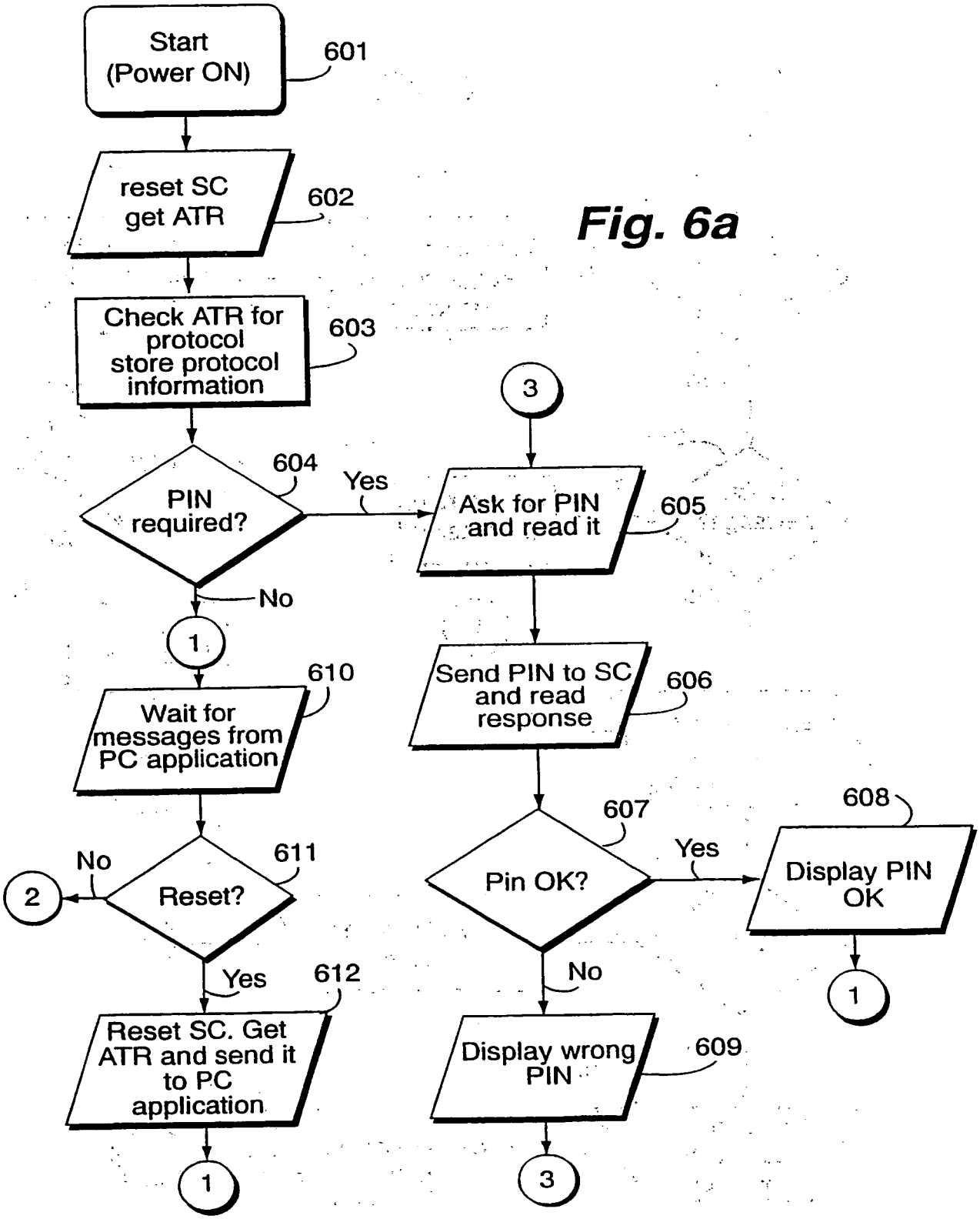

Start (Power ON)
601
reset SC get ATR
602
Check ATR for protocol store protocol information
603
PIN required?
604
Yes
No
Ask for PIN and read it
605
Send PIN to SC and read response
606
Pin OK?
607
Yes
No
Display PIN OK
608
Display wrong PIN
609
Wait for messages from PC application
610
Reset?
611
No
Yes
Reset SC. Get ATR and send it to PC application
612
1
2
3

Fig. 6a

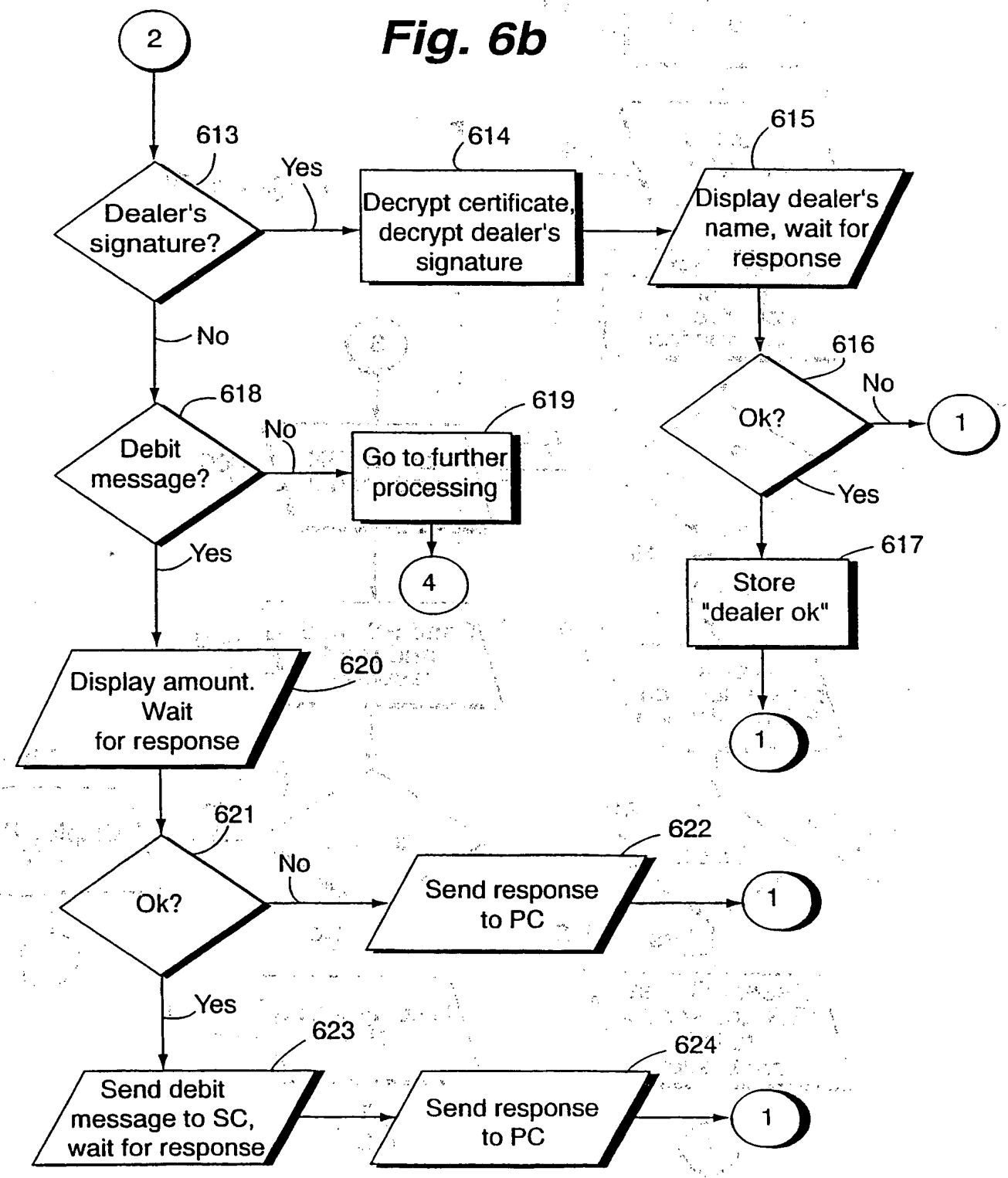
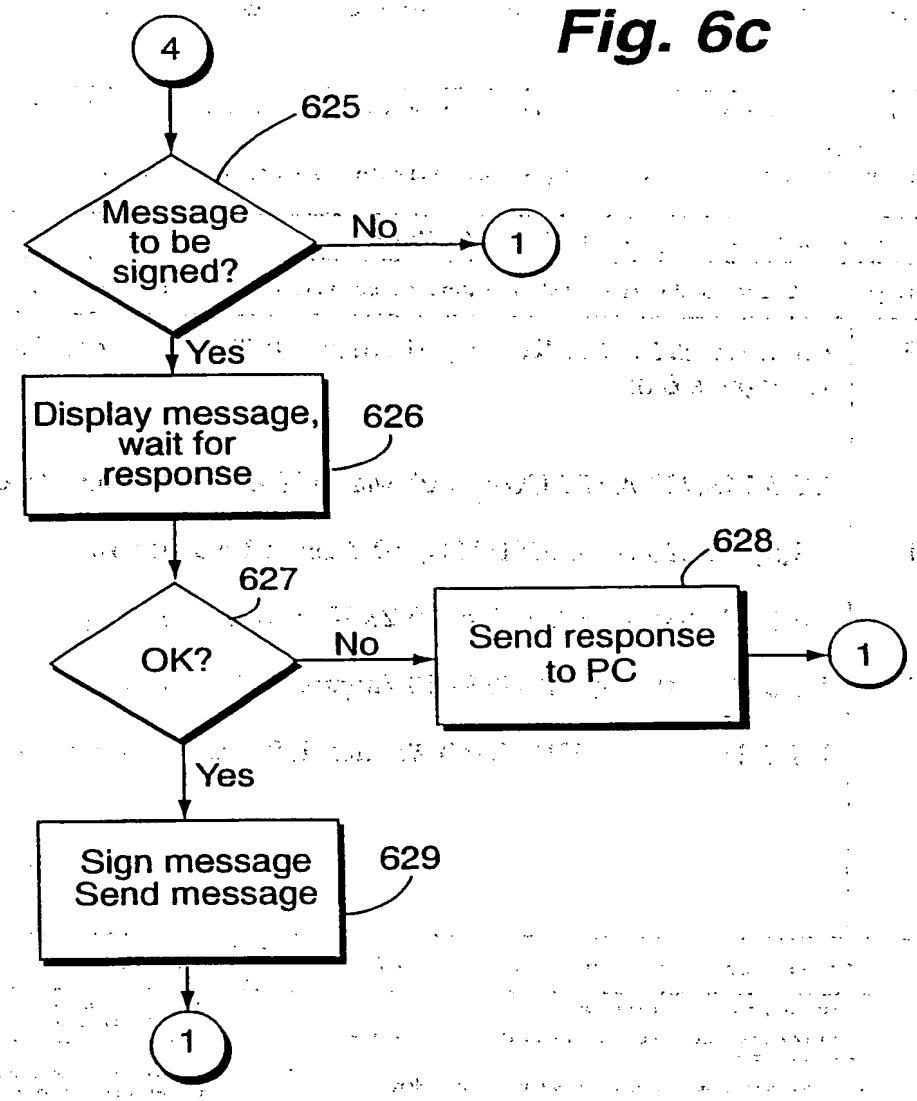

2
613
Dealer's signature?
Yes
614
Decrypt certificate, decrypt dealer's signature
615
Display dealer's name, wait for response
No
616
Ok?
No
1
Yes
618
Debit message?
No
619
Go to further processing
4
Yes
617
Store "dealer ok"
1
620
Display amount. Wait for response
621
Ok?
No
622
Send response to PC
1
Yes
623
Send debit message to SC, wait for response
624
Send response to PC
1

Fig. 6b

Fig. 6c


4
625
Message to be signed?
No
1
Yes
Display message, wait for response
626
627
628
OK?
No
Send response to PC
1
Yes
Sign message Send message
629
1

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/25584

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :G06F 17/60; G06K 5/00, 19/06, 19/07; H04L 9/00, 17/02; H04K 1/00

US CL :235/279, 380, 487, 492, 493; 380/23, 24, 25, 49, 52

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 235/279, 380, 487, 492, 493; 380/23 24, 25, 49, 52

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

STN, WEST
search terms: housing, numeric key, display, digital signature, memory card, smart card

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y, P	US 5,945,652 A (OHKI et al) 31 August 1999, col. 7, col. 10; col. 12; figures 6-8;	1-13, 20-22
Y	US 5,748,737 A (DAGGAR) 05 May 1998, col. 10, lines 45-65	1-3, 8-9, 11-13
Y, P	US 5,936,226 A (AUCSMITH) 10 August 1999, figures 1-4	4, 21, 22
Y	US 5,471,038 A (EISELE et al) 28 November 1995, figure 1	5
Y, P	US 5,936,149 A (FISCHER) 10 August 1999, figure 1	10
Y	US 5,221,838 A (GUTMAN) 22 June 1993, col. 2; figures 2B	6, 7

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 07 JANUARY 2000	Date of mailing of the international search report 10 FEB 2000
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer JAMES P. TRAMMELL Telephone No. (703) 305-9768

Form PCT/ISA/210 (second sheet)(July 1992) *

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/25584

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,815,577 A (CLARK) 29 September 1998, col. 3; col. 4; col. 5	14-20
Y	US 5,334,823 A (NOBLETT, JR. et al) 02 August 1994, col. 19-22; figures 3-4.	14-19